

ARMY, MARINE CORPS, NAVY, AIR FORCE



**AIR LAND SEA
APPLICATION
CENTER**

JTF-IM

MULTISERVICE PROCEDURES FOR JOINT TASK FORCE- INFORMATION MANAGEMENT

**FM 101-4
MCRP 6-23A
NWP 3-13.1.16
AFTTP(I) 3-2.22**

APRIL 1999

DISTRIBUTION RESTRICTION: Approved
for public release; distribution is unlimited.

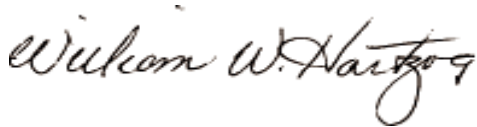
MULTISERVICE TACTICS, TECHNIQUES, AND PROCEDURES

Report Documentation Page

Report Date 00 Apr 1999	Report Type N/A	Dates Covered (from... to) -
Title and Subtitle Multiservice Procedures for Joint Task Force Information Management (JTF-IM)		Contract Number
		Grant Number
		Program Element Number
Author(s)		Project Number
		Task Number
		Work Unit Number
Performing Organization Name(s) and Address(es) HQ TRADOC Attn: ATDO-A Fort Monroe Va 23651-5000		Performing Organization Report Number
Sponsoring/Monitoring Agency Name(s) and Address(es)		Sponsor/Monitor's Acronym(s)
		Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes The original document contains color images.		
Abstract		
Subject Terms		
Report Classification unclassified	Classification of this page unclassified	
Classification of Abstract unclassified	Limitation of Abstract UU	
Number of Pages 74		

FOREWORD

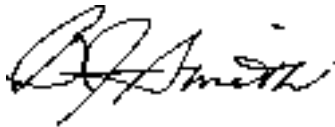
This publication has been prepared under our direction for use by our respective commands and other commands as appropriate.



WILLIAM W. HARTZOG
General, USA
Commander
Training and Doctrine Command



J. E. RHODES
Lieutenant General, USMC
Commanding General
Marine Corps Combat
Development Command



B. J. SMITH
Rear Admiral, USN
Commander
Navy Warfare Development Command



TIMOTHY A. KINNAN
Major General, USAF
Commander
Headquarters Air Force Doctrine Center

PREFACE

1. Scope

This publication provides multiservice tactics, techniques, and procedures (MTTP) for establishing an organized and disciplined approach for information management (IM) at the joint task force (JTF). It provides a “scheme of maneuver” for managing information. It provides a variety of options the JTF headquarters (HQ) information management officer (IMO) may use in developing a JTF information management plan (IMP).

2. Purpose

This publication provides the JTF tactics, techniques, and procedures (TTP) for effective and efficient distribution, control, and protection of information. It provides TTP for filtering, fusing, and prioritizing information enabling the commander to anticipate changing battlespace conditions, establish priorities, and facilitate decisionmaking.

3. Application

The audience for this publication includes commanders, staffs, and agencies at all levels within and supporting a JTF. It can serve as a source document for developing joint and service manuals, publications, and curricula or as a stand-alone document at the JTF and component levels. Using this publication assists the JTF in the effective and efficient use of available resources. Furthermore, this publication enhances the 2.0, 3.0, 5.0, and 6.0 series of joint publications, providing insight into the procedures for effective and efficient management of information. While written to a JTF level audience, this publication applies to any organization concerned with improving the flow and quality of information.

4. Implementation Plan

Participating Service command offices of primary responsibility (OPRs) will review this publication, validate the information, and reference and incorporate it in Service manuals, regulations, and curricula as follows:

Army. The Army will incorporate the procedures in this publication in United States (US) Army training and doctrinal publications as directed by the commander, US Army Training and Doctrine Command (TRADOC). Distribution is in accordance with DA Form 12-99-R.

Marine Corps. The Marine Corps will incorporate the procedures in this publication in US Marine Corps training and doctrinal publications as directed by the commanding general, US Marine Corps Combat Development Command (MCCDC). Distribution is in accordance with MCPDS.

Navy. The Navy will incorporate these procedures in US Navy training and doctrinal publications as directed by the commander, Navy Warfare Development Command (NWDC). Distribution is in accordance with MILSTRIP Desk Guide and NAVSOP Publication 409.

Air Force. Air Force units will validate and incorporate appropriate procedures in accordance with applicable governing directives. Distribution is in accordance with AFI 33-360.

5. User Information

a. The TRADOC-MCCDC-NWDC-AFDC Air Land Sea Application (ALSA) Center developed this publication with the joint participation of the approving Service commands. ALSA will review and update this publication as necessary.

b. This publication reflects current joint and Service doctrine, command and control (C2) organizations, facilities, personnel, responsibilities, and procedures. Changes in Service protocol, appropriately reflected in joint and Service publications, will likewise be incorporated in revisions to this document.

c. We encourage recommended changes for improving this publication. Key your comments to the specific page and paragraph and provide a rationale for each recommendation. Send comments and recommendation directly to—

Army

Commander
US Army Training and Doctrine Command
ATTN: ATDO-A
Fort Monroe VA 23651-5000
DSN 680-3153 COMM (757) 727-3153

Marine Corps

Commanding General
US Marine Corps Combat Development Command
ATTN: C42
3300 Russell Road
Quantico VA 22134-5021
DSN 278-6234 COMM (703) 784-6234

Navy

Navy Warfare Development Command (Det Norfolk)
ATTN: ALSA Liaison Officer
1540 Gilbert Street
Norfolk VA 23511-2785
DSN 565-0563 COMM (757) 445-0563
E-mail: ndcjoint@nctamslant.navy.mil

Air Force

Headquarters Air Force Doctrine Center
ATTN: DJ
216 Sweeney Blvd, Suite 109
Langley AFB VA 23665-2722
DSN 574-8091 COMM (757) 764-8091
E-mail: afdc.dj@langley.af.mil

ALSA

ALSA Center
ATTN: Director
114 Andrews Street
Langley AFB VA 23665-2785
DSN 575-0902 COMM (757) 225-0902
E-mail : alsadirector@langley.af.mil

**FM 101-4
MCRP 6-23A
NWP 3-13.1.16
AFTTP(I) 3-2.22**

FM 101-4	US Army Training and Doctrine Command Fort Monroe, Virginia
MCRP 6-23A	Marine Corps Combat Development Command Quantico, Virginia
NWP 3-13.1.16	Navy Warfare Development Command Newport, Rhode Island
AFTTP(I) 3-2.22	Headquarters Air Force Doctrine Center Maxwell Air Force Base, Alabama

8 April 1999

JTF-IM

Multiservice Procedures for Joint Task Force-Information Management

TABLE OF CONTENTS

	Page
EXECUTIVE SUMMARY	vi
CHAPTER I OVERVIEW FOR INFORMATION MANAGEMENT	
Background	I-1
IM and Decisionmaking	I-1
Information Management Plan (IMP)	I-2
Information Quality Characteristics	I-2
Cognitive Hierarchy	I-2
Information Flow	I-4
CHAPTER II DUTIES AND RESPONSIBILITIES	
Background	II-1
JTF HQ's Responsibilities	II-3
Information Management Board (IMB)	II-4
JTF Common Tactical Picture Board (CTPB)	II-5

	JTF IMO	II-5
	Staff Section IMO	II-5
	JTF Component and Supporting Agencies	II-5
	JTF Information and Information System User Responsibilities	II-6
	JTF Network Management Responsibilities	II-6
	JTF Information and Information System Protection Responsibilities	II-6
CHAPTER III	INFORMATION MANAGEMENT SYSTEMS	
	Background	III-1
	Global Command and Control System (GCCS)	III-1
	Network Application Management	III-3
	LAN	III-11
	AUTODIN Message Communications	III-11
	VTC	III-11
	Global Broadcasting System (GBS)	III-12
	Priority of Communication Means	III-13
CHAPTER IV	INFORMATION MANAGEMENT REQUIREMENTS, PROCESSES, AND PROCEDURES	
	Background	IV-1
	CCIR	IV-1
	RFI	IV-1
	CTP Management	IV-4
	Collaborative (Integrated) Planning System (CPS)	IV-4
	Joint Operations Center/Joint Intelligence Support Element Assessment Cell (JAC)	IV-5
	JTF Daily Operations Cycle (Battle Rhythm)	IV-6
	Reports Development	IV-7
	Orders	IV-10
	Briefings and Meetings	IV-11
	Internal Policies and Procedures	IV-12
	Multinational Procedures	IV-13
CHAPTER V	INFORMATION AND INFORMATION SYSTEM PROTECTION	
	Background	V-1
	Threats to IM	V-1
	Defensive Information Operations	V-2
	Information Destruction	V-4
REFERENCES	References-1
GLOSSARY	Glossary-1
INDEX	Index-1
FIGURES	I-1 Information Quality Criteria	I-3
	I-2 Cognitive Hierarchy	I-3
	II-1 Generic JTF Structure	II-2

II-2	JTF Staff Organization	II-2
II-3	Information Exchange Systems	II-3
III-1	COP Flow Chart	III-2
III-2	Sample JTF Home Page	III-4
III-3	Sample JTF Command Group Home Page	III-4
III-4	Sample JTF Component Home Page	III-5
III-5	Sample Major Unit Home Page	III-5
IV-1	Request for Information Flow Chart	IV-2

TABLES

III-1	Common Information Capabilities	III-1
III-2	Example JTF Newsgroup Home Page	III-6
III-3	JTF Newsgroups	III-7
III-3	JTF Newsgroups (Continued)	III-8
III-4	JTF Common Relevant Information	III-9
III-5A	JTF Shared Message Folders	III-10
III-5B	JTF Shared Message Folders	III-10
IV-1	RFI Tracking Log	IV-4
IV-2	Sample JTF HQ Daily Operations Cycle	IV-7
IV-3	JTF Reports Matrix (1 of 3)	IV-8
IV-3	JTF Reports Matrix (2 of 3)	IV-9
IV-3	JTF Reports Maxtris (3 of 3)	IV-10
IV-4	Sample JOC Message Log	IV-14
IV-5	Sample Master Suspense Action Log	IV-14
IV-6	Sample JTF Significant Events Log	IV-15
IV-7	Sample JTF Phone and E-Mail Directory	IV-15

EXECUTIVE SUMMARY

JTF-IM

Multiservice Procedures for Joint Task Force-Information Management

This publication—

- **Defines and outlines IM terms and processes to include filtering, fusing, and prioritizing.**
- **Outlines IM responsibilities for handling, managing, preserving, and protecting information.**
- **Provides an overview of systems available for supporting information management.**
- **Provides techniques on how to manage the vast amounts of information generated by different processes and systems (that is, electronic mail [e-mail], newsgroups, home pages, the Global Command and Control System [GCCS], official message traffic, and intelligence feeds).**
- **Provides tactics, techniques, and procedures to manage the information flow between the joint operations center (JOC) and the joint intelligence support element (JISE).**
- **Provides guidelines on managing the information pertaining to commander's critical information requirements (CCIR), requests for information (RFI) procedures, reports, briefings, and operations orders.**

Overview For Information Management

Chapter I introduces the definition and purpose of IM. It describes how IM relates to the JTF commander's decisionmaking process. It explains the relationship between this publication and a specific JTF information management plan. The chapter describes the general characteristics of information and information use supporting the commander's decisionmaking process. It concludes with a discussion on information flow in the JTF and defines the terms filtering, fusing, and prioritizing in the context of IM.

Duties and Responsibilities

Chapter II provides a delineation of positions/cells/sections and their IM responsibilities. It identifies the principal managers of the IM system while providing some definition of their broad responsibilities and their relationship to the JTF staff.

Information Management Systems

Chapter III discusses some IM systems available to the JTF staff and backup processes or systems for emergencies. It discusses managing information through GCCS, newsgroups, e-mail, and shared network drives to ensure it is available upon demand without crippling the information flow.

Information Management Requirements, Processes, and Procedures

Chapter IV provides guidelines on how to best manage the information generated by e-mail, GCCS, message traffic, etc. It also provides procedures for CCIR, RFI, and provides techniques on the management of reports, briefings, and operation orders.

Information and Information System Protection

Chapter V describes information assurance considerations such as the vulnerability to viruses, the levels of protection and defense, and the mechanisms that must be in place to prevent the user from short cutting or by-passing levels of protection. Information assurance also addresses safeguarding information.

PROGRAM PARTICIPANTS

The following commands and agencies participated in the development of this publication:

Joint

Joint Warfighting Center Fenwick Rd Bldg 96, Fort Monroe, VA 23651-5000
JTF-Bravo, APO AA 34042
Joint Special Operations Forces Institute, PO Box 71929, Fort Bragg, NC 28307-1929
Joint Staff, J-7, JDD 7000 Joint Staff, Pentagon Room 2B865, Washington, DC 20318-7000
Joint Staff, J-6, 6000 Joint Staff, Pentagon Room 2B865, Washington, DC 2038-6000
USACOM, (J2 and J353) 1562 Mitscher Avenue, Suite 200, Norfolk, VA 23551-2488
USACOM, JTASC (J646, J724, J75), 116 Lakeview Parkway, Ste 100, Suffolk, VA 23435-2697
USCENTCOM (CCJ5-O), 7115 S. Boundary Blvd, MacDill AFB, FL 33621-5101
USEUCOM (EJ5-D), Unit 30400, Box 1000, APO, AE 09128
USPACCOM (J383), Box 64013, Camp HM Smith, HI 96861-4013
USSOUTHCOM (SCJ5-PS), 3511 NW 91st Ave, Miami, FL 33172-1271
USSPACECOM (SPJ5X), 250 S. Peterson Blvd Suite 116, Peterson AFB, CO 80914-3130
USSTRATCOM (J512), 901 SAC Blvd, Suite 2E18, Offutt AFB, NE 68113-6500
USTRANSCOM, 508 Scott Dr, Scott AFB, IL 62225-5357
HQ USSOCOM (AOJ6-PS), 7701 Tampa Point Blvd, MacDill AFB, FL 33621-5323

Army

HQ TRADOC (ATDO-A), Ingalls Rd, Bldg 133 Room 7, Fort Monroe, VA 23651-5000
HQDA, ODCSOPS(DAMO-SSP), 400 Army Pentagon, Washington, DC 20310-0400
HQ XVIII ABN Corps, Fort Bragg, NC 28307-5000

Marine Corps

Marine Corps Combat Development Command, Joint Doctrine Branch (C427), 3300 Russell Rd, 3rd Floor Suite 318A, Quantico, VA 22134-5021
HQ US Marine Corps Strategy and Plans Division, Room 5D 616, Washington, DC 20380-1775
MARFORLANT Standing Joint Task Force (SJTF), Camp Lejeune, NC 28542
MCCDC, MAGTF Staff Training Program, (MSTP) (C54), Quantico, VA 22554

Navy

Navy Warfare Development Command, Det Norfolk, 1540 Gilbert Street, Norfolk, VA 23511-2785
CINCLANTFLT, 1562 Mitscher Ave, Ste 250, Norfolk, VA 23511-2487
Chief of Naval Operations (N512), Department of the Navy, Washington, DC 20350-2000
2nd Fleet, FPO AE 09506-6000
2nd Fleet, DECOMUSNAVCENT, 2707 Zemkeave, MacDill AFB FL 35621-5105

Air Force

HQ Air Force Doctrine Center (AFDC), 155 N. Twining Street, Maxwell AFB, AL 36112
AFDC Detachment 1, 216 Sweeny Blvd, Ste 109, Langley AFB, VA 23665
HQ AFCENT, 460 Box 539, APO AE 09703
HQ USAFE/SCE, APO AE 09094
HQ ACC/DOI/INOUS/SSSD/ASC2A, Langley AFB, VA 23665
HQ 3AF/CCEA, PSC 37 Box 1, APO AE 09459
HQ 8 AF /SC/AS, Barksdale AFB, LA 71110-2279
HQ 9 AF, 524 Shaw Drive, Shaw AFB, SC 29152-5029
HQ 12 AF, Davis-Monthan AFB, AZ 85707-4100
608 Air Opns Group, 245 E. Davis Blvd, Room 246, Barksdale AFB, LA 71110

Other

HQ US Coast Guard (G-OPD), 2100 2nd Street SW, Room 3121, Washington,
DC 20593-0001

OVERVIEW FOR INFORMATION MANAGEMENT

The Joint Campaign should fully exploit the information differential, that is, the superior access to and ability to effectively employ information on the strategic, operational, and tactical situation which advanced U.S. technologies provide our forces.

Joint Pub 1

1. Background

Information management (IM) refers to the processes a joint task force (JTF) uses to obtain, manipulate, direct, and control information. IM includes all processes involved in the creation, collection and control, dissemination, storage and retrieval, protection, and destruction of information. The goal of IM is providing a timely flow of quality information enabling the commander, joint task force (CJTF) to anticipate and understand the consequences of changing conditions. This publication provides the JTF headquarters (HQ) a variety of techniques to manage information efficiently.

2. IM and Decisionmaking

a. Skillful decisionmaking is central to the art of command. Judgement, experience, and vision are some of the factors facilitating skillful decisionmaking. Perhaps the paramount factor is situational awareness. Awareness and understanding of the operational environment allows the CJTF to anticipate future conditions, formulate concepts of operations, analyze courses of action, and accurately assess risks. For years, commanders made decisions based on where they understood the threat to be relative to their forces. The staff depicted on map boards and overlays information necessary to plan, execute, and

assess operations. This graphic depiction of the battlespace enhanced with text files (messages, reports, etc.) provided the commander a common tactical picture (CTP). Often graphic and text information combined with the commander's experience (intuitive reasoning) enabled the commander to make sound and timely decisions.

b. Technology. Technology is changing and automating the age-old method of achieving a CTP. Simultaneous distribution of planning cell information to multiple units is a reality. Today JTFs display in a more automated dynamic manner friendly and threat air, ground, surface, and subsurface unit locations and status. An automated display helps the JTF maintain a more timely and accurate CTP and allows the commander to develop enhanced situational awareness of the operating environment.

c. Automated Systems. Today, commanders and staffs rely on a variety of automated systems to meet information requirements. The advances in communications and computing equipment place enormous amounts of information virtually at the commander's fingertips. The success of these systems is also the downfall of the systems' approach. More information is available than most humans have the capacity to assimilate, collate, and evaluate. Commanders are becoming victims to system success by losing control of the information needed to support their decisionmaking processes.

d. Situational Awareness. Information systems continue to play an important role in building situational awareness. Two principal considerations help to improve the utility of these systems in supporting the decisionmaking process. First,

information users at all levels need to change the way they think about information. Instead of thinking of information in terms of systems, think of information as a commodity. Consider information as an input to the decision-making process. This assists the staff in focusing on what the commander needs, when it is needed, and presenting it in a usable format to complete the decision-making process. Second, the JTF must develop a plan for managing information. This ensures that the required information is available in each process leading to required decisions.

3. Information Management Plan (IMP)

The introduction of ambiguous or incorrect information devalues the JTF HQ IM processes. This may be the result of incorrectly posting draft documents as approved documents or posting information in the wrong location, causing uncertainty and a loss of accurate situational awareness. Information managers reduce the risk of introducing uncertainty and ambiguity by developing a comprehensive IMP employing effective records management processes.

a. IM requirements vary, and this publication can not cover all of the possibilities. Therefore, a JTF must develop an IMP tailored to manage information within the context of their mission and capabilities. An effective IMP provides guidance ensuring the availability of “quality information” throughout the JTF HQ. The CJTF can then correctly assess changing conditions, establish priorities, and facilitate the decisionmaking process.

b. The JTF IMP should cover JTF unique IM needs. These include the duties, responsibilities, and skill requirements; IM systems and requirements; IM processes and procedures; and IM system protection. The JTF IMP should include specific guidance for the management of the JTF

CTP, collaborative (integrated) planning systems, request for information (RFI) management procedures, and network applications used to post JTF information. This guidance may include using news-groups, web pages, or other applications.

c. The development and execution of an effective JTF HQ IMP requires the participation and interaction of the CJTF, chief of staff, all staff sections, and the JTF’s components. The HQ should develop processes, procedures, pathways, and systems supporting each staff section once they identify their “information requirements.”

4. Information Quality Characteristics

Quality information adds value to JTF staff processes. Information is susceptible to distortion and deception. When developing the IMP, the information management officer (IMO) must consider the information quality characteristics outlined in Figure I-1.

5. Cognitive Hierarchy

Never forget that all technology can ultimately do is give your staff more time to think. It can't think for them. Data is not information. Information is not judgement. Judgement is not wisdom. Numbers aren't policy. Quantitative approaches can't solve qualitative problems.

Joshua Shapiro, Technology Consultant

a. Reducing uncertainty and increasing the CJTF’s situational awareness are the focus of IM processes. IM processes use data and information that have been processed or displayed in a form that is understandable to the personnel using them to enhance situational awareness. We use the term information generically to refer to everything from data on the one hand to knowledge and understanding on the other. It is important to recognize there are four classes of information (see Figure I-2).

ACCURACY

Information that conveys the true situation.

RELEVANCE

Information that applies to the mission, task, or situation at hand.

TIMELINESS

Information that is available in time to make decisions.

USABILITY

Information that is in common, easily understood format and displays.

COMPLETENESS

Necessary information required by the decisionmaker.

BREVITY

Information that has only the level of detail required.

SECURITY

Information that has been afforded adequate protection where required.

Figure I-1. Information Quality Criteria

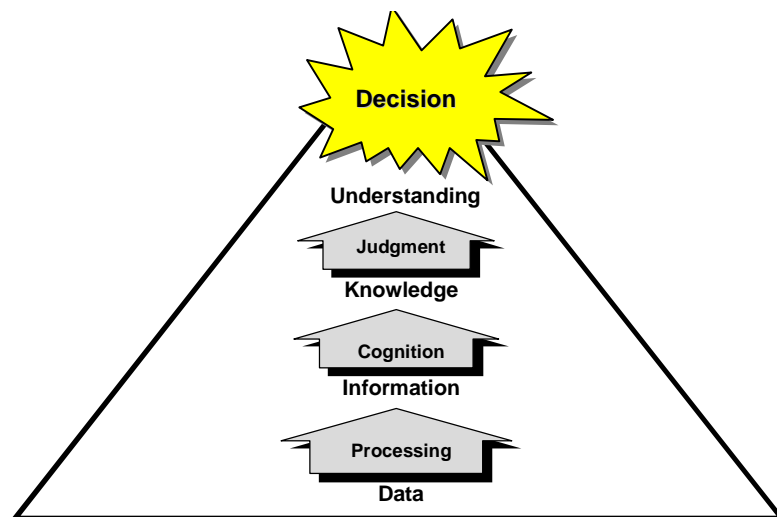


Figure I-2. Cognitive Hierarchy

(1) Data. Data is the facts and individual data that are the building blocks of information.

(2) Information. Information is the result of organizing, collating, comparing, processing, analyzing, and filtering data.

(3) Knowledge. Knowledge is the result of correlating and fusing information and assessing its meaning through the application of cognition. You begin to build an accurate picture of the situation through integrating and interpreting various pieces of processed data. At this level, you are starting to get a product that can be useful for decisionmaking.

(4) Understanding. Understanding is highest class of information. Obtain "understanding" when you synthesize a body of knowledge and apply judgement to fill in the gaps to arrive at a complete image of the situation. An "understanding" of the situation provides situational awareness to anticipate future events and to make sound timely decisions.

b. The graduations between the different classes of information are not always clear. Little meaning or value is possible until data is integrated, interpreted, and placed in proper context. Knowledge is gained once information determining reliability, relevance, and importance is evaluated. The following example illustrates how you process data through the cognitive hierarchy resulting in high value understanding. At the *data* level, the JTF Manpower and Personnel Directorate (J-1) determines that JTF strength is 21,863 personnel. Analysis of this data derives the *information* that the JTF components are at combat strength. Fused with information regarding enemy capabilities, the CJTF makes a *knowledgeable* determination that the JTF has the personnel capability to execute a specific course of action. By applying judgement, the CJTF and staff can anticipate likely courses of action, gain situational awareness (*understanding*), and

can employ JTF combat power appropriately.

6. Information Flow

a. JTF HQ IM procedures must provide for the rapid flow, vertical and horizontal, of information. Most JTF HQ's staff processes require a cross-functional and cross-directorate exchange of information. Traditional staff arrangements help determine where information should flow within the organization, but these arrangements should not form firewalls to the information exchange. Effective flow of information within the various JTF processes requires the information to be—

(1) Positioned Properly. The JTF's need for specific types of information are often predictable. Positioning the required information at its anticipated points of need speeds the flow and reduces demands on communications systems (for example, using public folders to post required information).

(2) Mobile. The reliable and secure flow of information must be commensurate with the JTF's mobility and tempo of operations. Information flow must immediately adjust to support the vertical and lateral flow of information between adjacent forces (for example, collaborative [integrated] planning system).

(3) Accessible. All levels of command must be able to pull the information needed to support concurrent or parallel planning and mission execution. If possible, channel information to the required user via automated means reducing the need for manual exchange (for example, graphic depiction of forces in a CTP).

(4) Fused. We receive information from many sources, in many mediums, and in different formats. Fusion is the logical blending of information from multiple sources into an accurate, concise, and complete summary. The goal of IM is reducing information to the minimum

essentials and in an easily understood and acted on format (for example, threat assessment disseminated in graphic form on an automated CTP system).

b. The JTF's command, control, communications, computer, and information (C4I) systems provide the means for information dissemination. Users of the information are ultimately responsible for its management. Principal, special, and supporting staff directors or chiefs must clearly identify their information requirements and work closely with the JTF IMO, ensuring processes are automated in the most effective way possible.

c. The IMP should include procedures to filter, fuse, and prioritize required information. This publication discusses these concepts.

(1) Filtering is a process of organizing information based on specified criteria.

(2) Fusion assesses information from multiple sources and develops a concise and complete summary.

(3) Prioritization focuses the efforts of the JTF HQ on developing information supporting the CJTF's decisionmaking process.

d. Information flow within the JTF is a complex yet vital function for reducing uncertainty and ambiguity while facilitating a clear understanding of the battlespace for the commander. Optimum information flow within the JTF requires both speed and clarity of transfer without creating fragmented or useless information. The IMP should assign responsibilities and provide instructions on managing information for the JTF. This is a vital step ensuring decisionmakers have the required information, when they need it, and in an understandable format.

Information Management was the number one problem facing the JTF.

JULLS Long Report 21340-59252

DUTIES AND RESPONSIBILITIES

Information management is now viewed as a strategic enabler for achieving an organization's mission and economic health.

*National Academy of Public
Administration for DOD*

1. Background

This chapter identifies the principal managers of JTF IM and outlines some of their responsibilities. An organized and disciplined effort is necessary by all personnel to ensure an uninterrupted flow of information. Every user has inherent responsibilities to acquire, assess, reason, question, correlate, and disseminate quality information to other users. All JTF personnel, as information users, are also information managers. As information users, each member of the JTF must continuously ask the following three questions:

a. Does the information already exist? Time is wasted developing information (point papers, briefings, etc.) if the information already exists. Responding to multiple requests for the same information is wasted effort. One solution is developing a collaborative (integrated) planning system that supports information requirements necessary to support planning, decisionmaking, execution, and assessment.

b. Who else needs the information? Sharing information is essential to maintain unity of effort and synchronization of operations. Users must consider who (higher, lower, and laterally) requires the information to assist in developing solutions. Figure II-1 depicts the structure

of a generic JTF and its components. Figure II-2 depicts a JTF staff organization.

c. What is the most efficient and effective way to transfer the information? Many times the initial reaction to receipt of seemingly important information is sending an electronic mail (e-mail) to "all JTF staff." Newsgroups, web sites, and public folders are increasingly popular methods for transferring important information. However, posting information to a newsgroup, homepage, or public folder is no guarantee of receipt by the intended audience. Understanding the "process" (information flow) that satisfies each essential JTF requirement enables all personnel to determine the most efficient and effective means to transfer information. A few moments of consideration assists in determining what is the best, most timely, efficient, and effective method of notifying the appropriate JTF staff members. Consideration must be given to whether using newsgroups, web sites, or public folders are timely for critical actions such as transmitting fragmentary orders (FRAGOs) or warning orders. Occasionally, direct contact is a more appropriate means. Figure II-3 depicts the matching of some information exchange systems to their intended audience.

A host of other computer-based systems and equipment may be used to exchange information including radio, telephone, e-mail, push technology, Automatic Digital Network (AUTODIN), Defense Message System (DMS), on-line chat, video teleconferencing (VTC), etc. The dependency of the JTF on automated systems increases the exploitation value of these systems by the enemy.

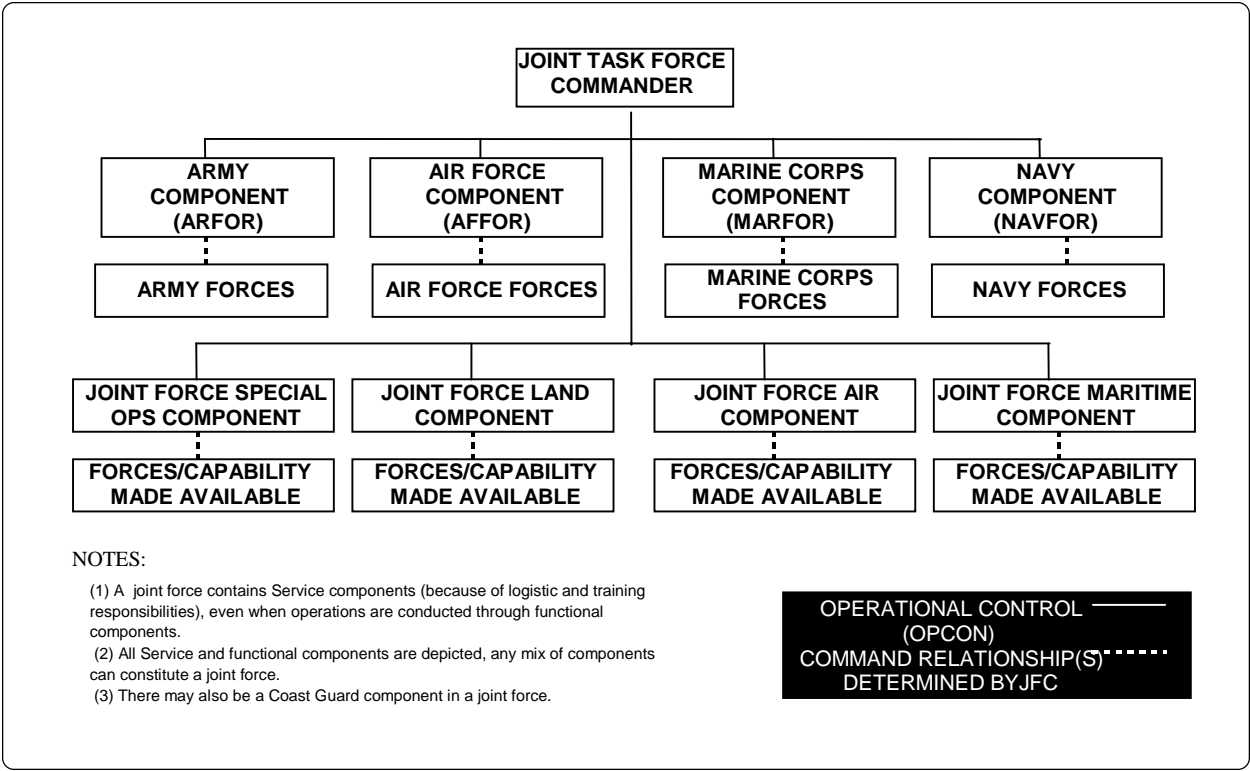


Figure II-1. Generic JTF Structure

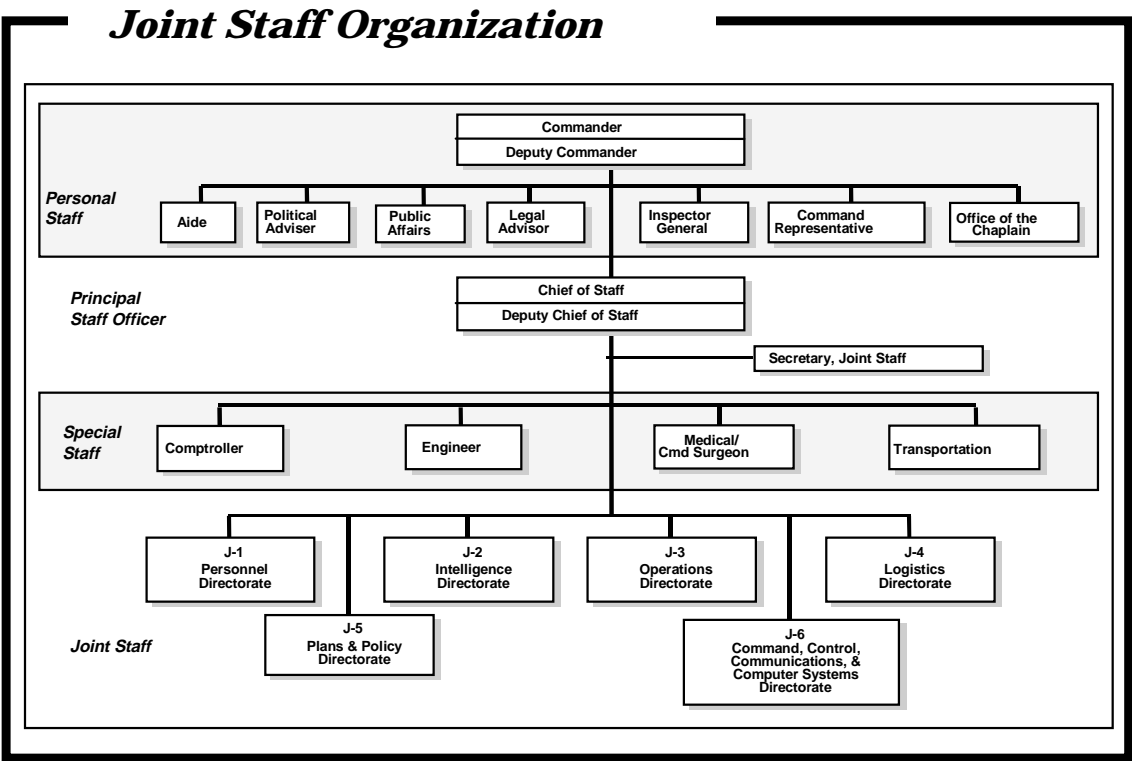


Figure II-2. JTF Staff Organization

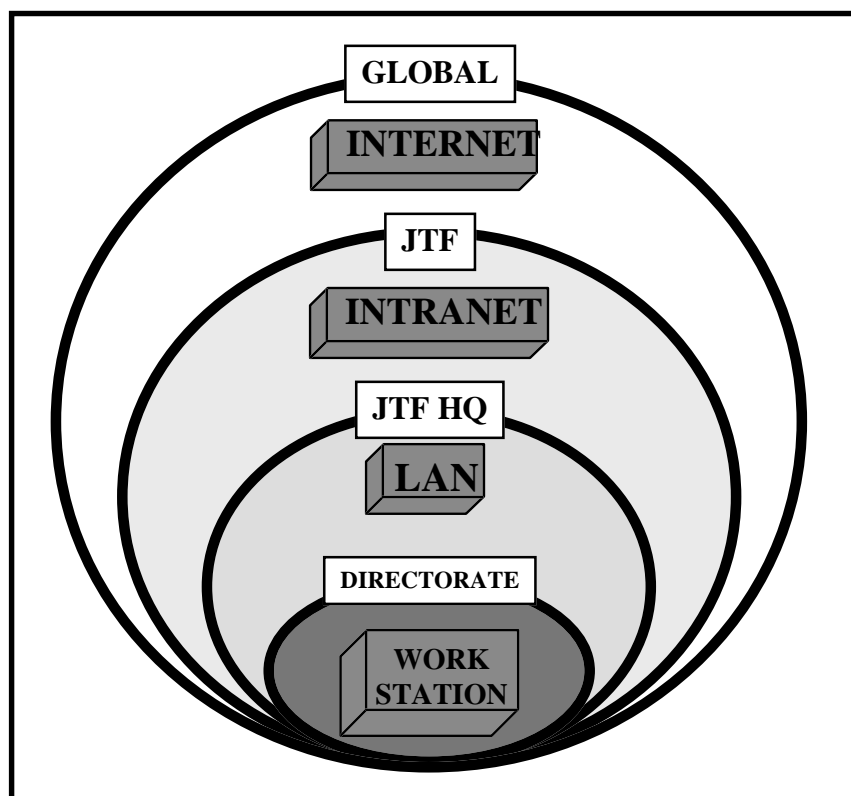


Figure II-3. Information Exchange Systems

2. JTF HQ's Responsibilities

a. CJTF. The CJTF—

(1) Establishes the priorities for information gathering and reporting by establishing the commander's critical information requirements (CCIR) outlined in Chapter IV.

(2) Approves the JTF HQ IMP.

(3) Approves the JTF communications plan that supports the IMP.

b. JTF Chief of Staff. The JTF chief of staff—

(1) Approves the JTF HQ daily operations cycle/battle rhythm, outlined in Chapter IV.

(2) Implements the JTF HQ IMP.

(3) Appoints the JTF IMO.

(4) Appoints a JTF web administrator and a JTF web grandmaster, if web technology is used.

(5) Approves format and structure of information posted and distributed from the JTF (that is, briefings, reports, etc.).

c. Principal JTF Staff Sections. The principal JTF staff sections—

(1) Establish internal staff section procedures for newsgroups, home pages, message handling, e-mail, RFI, and suspense control procedures.

(2) Appoint a staff section IMO as a point of contact for IM matters.

(3) If web technology is used, appoint a webmaster for their section.

(4) Ensure training on basic IM and security procedures for all directorate personnel.

(5) Assess IM to ensure quality and flow. Establish benchmarks or subjective analysis to evaluate efficiency and effectiveness of IM.

d. JTF Command, Control, Communications, and Computer Systems Directorate. The JTF J-6—

(1) Works closely with the JTF IMO to develop the JTF communications plan.

(2) Establishes a technical help desk for network and systems administration issues for information systems (for example, collaborative [integrated] planning system).

(3) Establishes e-mail accounts.

(4) Consolidates a list of communication's and system's requirements.

(5) Produces the JTF telephone and e-mail directories, outlined in Chapter IV.

(6) Establishes a central location and procedure for conducting virus scanning of incoming diskettes and laptops, outlined in Chapter V.

(7) Acts as office of primary responsibility (OPR) for managing networks and network services (number of newsgroups, access, etc.).

(8) Ensures system training and familiarization for JTF staff and augmentees.

e. Joint Operations Center (JOC). The JOC—

(1) Assesses the information flow to support JTF operations and monitors the efficiency, effectiveness, and accuracy of the JTF's CTP, outlined in Chapter IV.

(2) Maintains a master suspense action log, outlined in Chapter IV.

(3) Maintains a chronological record of JTF significant events, outlined in Chapter IV.

(4) Responsible for the CJTF's daily briefings and FRAGO production.

(5) Works closely with the joint intelligence support element (JISE) to assess, update, and integrate information requirements.

(6) Reviews and records incoming message traffic, outlined in Chapter IV.

f. JISE. The JISE—

(1) Reviews, assesses, and disseminates required threat information in text and/or graphic products to support the JTF CTP.

(2) Monitors the efficiency, effectiveness, and accuracy of the threat assessment displayed by the JTF CTP.

(3) Works closely with the JOC to assess, update, and integrate information requirements.

3. Information Management Board (IMB)

The IMB—

a. Acts as the focal point for coordinating IM within the JTF.

b. Convenes during the development of the JTF HQ IMP and as required thereafter.

c. Is headed by the JTF IMO.

d. Operates under the supervision of the chief of staff, or appropriate staff directorate, as best meets the JTF's mission needs.

e. Is composed of the senior IMO from each staff section, component, and supporting agency. If the JTF uses web technology, the IMB should also include the JTF web administrator, web grandmaster, and selected webmasters from each staff section, component, and supporting agency.

f. Is actively involved in resolving cross-functional and contentious IM issues.

4. JTF Common Tactical Picture Board (CTPB)

The CTPB—

a. Acts as the focal point for coordinating the CTP within the JTF.

b. Is headed by the JTF common tactical picture manager (CTPM), who is responsible for developing CTP procedures to maintain situational awareness of friendly and threat units.

c. Operates closely with the JTF IMO, the JOC and JISE watch officers, and appropriate staff directorates.

d. Is composed of the friendly air, land, sea, and threat force track managers.

e. Convenes as required.

f. Is actively involved in resolving all cross-functional CTP issues.

5. JTF IMO

The JTF IMO—

a. Develops and publishes the JTF HQ IMP, described in Chapter I.

b. Publishes the JTF HQ daily operations cycle/battle rhythm, outlined in Chapter IV.

c. Publishes the JTF reports matrix, outlined in Chapter IV.

d. Coordinates additional training requirements by staff and component elements to support IM.

e. Heads the IMB.

f. Works closely with the CTPM to develop effective, efficient track/location management procedures.

g. If web technology is used, works closely with the JTF web administrator, ensuring establishment of the JTF web site infrastructure facilitating the necessary information exchange throughout the JTF.

h. May be a commissioned or non-commissioned officer regardless of rank, specialty, or Service, as best meets the requirements of the JTF. However, selection should reflect the best use of trained personnel and existing expertise.

6. Staff Section IMO

The staff section IMO—

a. Oversees the internal and external information flow of their staff section.

b. Provides the JTF IMO with staff section information requirements for incorporation into the JTF IMP.

c. Provides the JTF J-6 a list of their requirements for network support.

d. Ensures compliance with the IMP for the establishment of newsgroups and/or web sites, message handling, e-mail, RFI, and suspense control procedures.

e. Coordinates/conducts internal IM training for staff section members.

f. May be commissioned or non-commissioned officers regardless of rank, specialty, or Service. However, selection should reflect the best use of trained personnel and existing expertise.

7. JTF Component and Supporting Agencies

If the JTF chooses to use a web site, each component and supporting agency should appoint a webmaster as a primary point of contact for web site technical matters. Each component and supporting agency should also appoint an IMO as a primary point of contact for IM matters. Component and supporting agency IMOs—

a. Review the JTF HQ's daily operations cycle/battle rhythm and IMP, outlined in Chapter IV.

b. Conduct liaison with the JTF IMO.

c. Coordinate and conduct IM training for members of the component or agency.

d. May be commissioned or non-commissioned officers regardless of rank, specialty, or Service. However, selection should reflect the best use of trained personnel and existing expertise.

8. JTF Information and Information System User Responsibilities

The JTF information and information system user responsibilities are to—

a. Ensure accuracy of JTF information.

b. Properly control, classify, protect, and archive all JTF information and information systems for which they are responsible.

c. Validate the authority to destroy JTF information before destruction.

d. Read and comply with the information requirements published in the JTF IMP.

9. JTF Network Management Responsibilities

If the JTF chooses to use web technology, four distinct roles to support this network technology must be identified and their responsibilities established: JTF web administrator, JTF web grandmaster, webmasters, and information producers.

a. JTF Web Administrator. The web administrator is responsible for the overall management of information on the JTF web site. The web administrator must coordinate with the various staff sections, components, and supporting agencies ensuring establishment of the web site

infrastructure facilitating the necessary information exchange throughout the JTF. The web administrator is not a technical role, although an understanding of web technology is required. The web administrator ensures maintenance of the posted information in accordance with the IMP. The JTF IMO may also be designated the web administrator.

b. JTF Web Grandmaster. The grandmaster must work very closely with the JTF administrator and the JTF IMO for the technical development of the JTF web site. The grandmaster coordinates the activities of the webmasters throughout the JTF.

c. Webmaster. By contrast, the webmaster is responsible for the technical infrastructure of the JTF web site to include templates and forms. The webmaster's primary responsibility is installing new network management technologies, management, and help their respective organization or staff section use them. The webmaster provides the tools enabling JTF users to publish, access, and customize information themselves rather than doing it all for them. The webmaster should assist in converting documents to appropriate HyperText Markup Language (HTML) format and ensure that HyperText Transfer Protocols (HTTP) remain current.

d. Information Producers. Each component, supporting agency, and JTF staff section, as producers of information, determines what information they create and maintain on the JTF web site. The information producer is responsible for keeping their portion of the JTF web site at their level and below current and accurate.

10. JTF Information and Information System Protection Responsibilities

a. Information Security Manager. The information security manager is responsible for the proper accountability, control, personnel access, and physical security/storage of noncompartmented

Department of Defense (DOD) classified data, in both hard and soft copy forms. This includes the TOP SECRET Control Officer's (TSCO's) responsibility for the JTF TOP SECRET registry's accountability, control, and access. The JTF appoints at least one TSCO, in either the JTF Manpower and Personnel Directorate (J-1) or Plans Directorate (J-5), and each JTF staff directorate normally appoints a security manager. See DOD 5200.1-R, *DOD Information Security Program*, 7 Jun 82, and applicable Service regulations for additional details.

b. Special Security Officer (SSO). The SSO is responsible for sensitive compartmented information (SCI) management, controls, and access. This publication is normally a JTF Intelligence Directorate (J-2) function.

c. Operations Security (OPSEC) Officer. The OPSEC officer is responsible for oversight and implementation of the JTF's OPSEC program. This position is normally a JTF Operations Directorate (J-3) function.

d. Designated Approving Authority (DAA). The DAA ensures, implements, and monitors a reliable information security (INFOSEC) program. The function of the DAA for all JTF information systems, with the exception of those systems processing SCI, is normally a responsibility of the JTF J-6. DAA for SCI information systems is handled via the SSO. The DAA has the following responsibilities:

- (1) Accredits all automated information systems (AISs) under their jurisdiction before placing them into operation.

- (2) Allocates resources (funding and manpower) to achieve and maintain an acceptable level-of-protection and to remedy security deficiencies.

- (3) Makes sure certifying officials, functional OPRs, and information systems security officers (ISSM) are identified for all AIS under their jurisdiction.

- (4) Approves system security policies.

e. ISSM. Normally a JTF J-6 function, the ISSM is the focal point and principal advisor for INFOSEC matters on behalf of the DAA. The ISSM has the following responsibilities:

- (1) Develops, implements, and maintains the JTF staff INFOSEC plan for all systems operated in the command.

- (2) Ensures information systems security officer (ISSO) and other information system (IS) security staff are properly trained and appointed in writing.

- (3) Assists ISSOs with preparing accreditation support documentation including risk assessment documentation, security test and evaluation (ST&E) documentation, and contingency plans.

- (4) Ensures that configuration management of staff hardware and software complies with the INFOSEC plan.

f. ISSO. The ISSO is normally a JTF J-6 responsibility. The ISSO is responsible for implementing and maintaining security on behalf of the ISSM. The ISSO reports to the JTF ISSM for INFOSEC matters and implements the overall INFOSEC program approved by the DAA. Each staff directorate in the JTF organization appoints in writing an ISSO. Larger directorates may appoint multiple ISSOs. They forward ISSO appointment letters to the ISSM. The ISSO is the point of contact for IS matters within their selected area of appointment, with the following responsibilities:

- (1) Develops a system security policy for AIS and networks that process or protect sensitive unclassified and classified information.

- (2) Makes sure that audit trails are reviewed periodically (for example, daily, weekly, etc.).

(3) Performs an initial evaluation of each vulnerability or incident, begins corrective or protective measures, and reports according to established network incidents reporting procedures.

(4) Notifies the DAA when AIS are involved.

(5) Evaluates known vulnerabilities to ascertain if additional safeguards are needed.

(6) Coordinates with the ISSM on matters concerning INFOSEC.

(7) Ensures IS security procedures are implemented within their assigned area.

(8) Ensures users within assigned areas are operating, maintaining, and disposing of systems per INFOSEC policies and procedures.

(9) Trains the IM users within the assigned area on INFOSEC responsibilities.

(10) Ensures personnel and physical security requirements are followed.

g. Network Security Officer (NSO). The NSO is normally a JTF J-6 function. The NSO is responsible for implementing and maintaining network security on behalf

of the ISSM. The J-6 appoints the NSO, who has the following responsibilities:

(1) Ensures incorporation of countermeasures and safeguards in the network design and daily performance of the network.

(2) Informs the ISSM of external network connection requirements so the ISSM can request memorandums of agreement (MOAs).

(3) Develops and promulgates the standard INFOSEC procedures governing network operations.

(4) Ensures security measures and procedures used at the network nodes fully support the security integrity of the network.

h. Terminal Area Security Officers (TASO). When needed, the officer-in-charge for each remote site, with a terminal connection to a network, designates a TASO in writing. The TASO is the representative of the ISSM or ISSO in matters pertaining to the security of each terminal. Each JTF HQ's staff directorate operating both a classified and unclassified network terminal normally appoints TASOs. The TASO enforces all applicable security requirements implemented by the INFOSEC program and the ISSM.

INFORMATION MANAGEMENT SYSTEMS

We owe the men and women who may be in harm's way every edge technology can provide. Technology will never be a substitute for courage and human toughness in conflict, but it can increase the likelihood that the tough and the courageous will be successful.

*Admiral William A. Owens,
Vice Chairman, Joint Chiefs of Staff*

1. Background

The goal of information systems and IM procedures is producing an accurate picture of the battlespace and supporting decision-making. Information systems must provide effective and secure information exchange throughout the JTF. Table III-1 provides a brief summary of some information systems currently available. Users need to develop an understanding of the information systems available and develop IM procedures to match their information requirements.

2. Global Command and Control System (GCCS)

GCCS is one of the IM systems used by a JTF. GCCS is a comprehensive, world-wide system providing information processing and dissemination capabilities necessary to conduct command and control (C2) of joint forces. This system improves visibility of the operational environment and with commonly understood "procedures" enhances situational awareness. There are four primary software modules within GCCS providing critical information flow to enhance situational awareness. The Joint Operations Planning and Execution System (JOPES), Joint Deployable Intelligence Support System (JDISS), common operational picture (COP) segment (chart)/common tactical picture (CTP), and a software package with a browser application program with e-mail and newsgroup capabilities. Basic descriptions of each module follows:

Table III-1. Common Information Capabilities

	GCCS	Web Pages/Newsgrups	E-mail	Local Area Network
Visibility	Sender and receiver(s) in the GCCS community	Broadcast within the SIPRNET community	Sender and receiver(s)	Local area network users at JTF HQ
Uses	<ul style="list-style-type: none"> •Official for record e-mail •Updating the COP •Formal traffic •Conducting dialog and coordinating actions 	<ul style="list-style-type: none"> •Information for record •COA •OPLAN •RFI •Other final products, official positions, and decisions 	<ul style="list-style-type: none"> •Informal and formal dialog •Resolving and negotiating differences •Private or group recipients •External file transfer 	<ul style="list-style-type: none"> •Staff coordination •Working documents •Local SOP, schedules, etc. •Internal file transfer
Similar To	<ul style="list-style-type: none"> •Telephone or conference call •Coordinating official actions •AUTODIN 	<ul style="list-style-type: none"> •Publishing an article in the newspaper •Establishing an official position •Bulletin board 	<ul style="list-style-type: none"> •Telephone or conference call •Informal memorandum 	<ul style="list-style-type: none"> •Circulating a written draft for review and coordination •Local issues •Staff input
Purpose	One-to-one or one-to-many communications	One-to-many or one-to-all communications	One-to-one or one-to-many communications	One-to-few or many-to-many communications

a. **JOPEs.** JOPEs supports military planning, deployment, execution, redeployment, and operations monitoring. JOPEs incorporates policies, procedures, personnel, and facilities by interfacing with automatic data processing (ADP) systems and reporting systems providing support to senior level decisionmakers and their staffs with the capability to plan and conduct joint military operations. (Submit movement requirements to United States Transportation Command [USTRANSCOM] using JOPEs procedures and ADP systems.) Information regarding crisis action planning is contained in Chairman of the Joint Chief of Staff Manual (CJCSM) 3122.01, JOPEs Volume I, *Planning Policies and Procedures*, Chapter V. Specific guidance for the format and content of operations plans/orders (OPLANs/OPORDs) are provided in CJCSM 3122.03, JOPEs Volume II, *Planning Formats and Guidance*, Chapter III. The model in Chapter III illustrates the format of an OPLAN/OPORD and outlines the information and instructions included in each plan element.

b. **JDISS.** JDISS is a transportable workstation and communications system electronically extending a theater Joint Intelligence Center (JIC) to a JTF or other tactical users. JDISS requires a common SECRET Internet Protocol Router Network (SIPRNET) network or Joint Worldwide Intelligence Communications System (JWICS) network, depending on classification. SIPRNET supports SECRET information requirements; JWICS supports SCI information requirements. JDISS is the primary source for intelligence reporting, database access, access to the intelligence RFI system, the Community On-line Intelligence System for End-Users and Managers (COLISEUM). JDISS provides automation to pull information from other theater and national intelligence databases.

c. **COP.** Figure III-1 depicts a skeleton outline of the COP process. The development and maintenance of the COP requires the JTF and all components adherence with established COP procedures and the procedures explained in Chapter IV. The

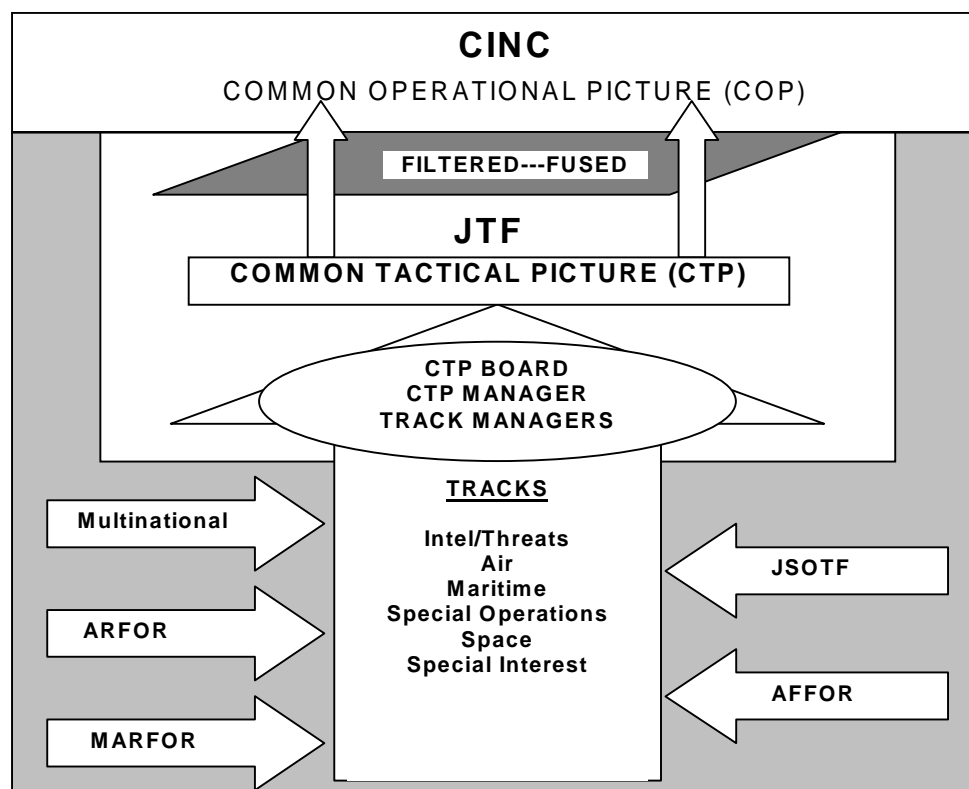


Figure III-1. COP Flow Chart

JTF's CTP feeds the commander in chief (CINC) COP. Component reporting systems provide friendly and threat air, maritime, and ground locations/tracks. The COP provides commanders with a near-real-time force tracking mechanism.

d. Software Package. Currently GCCS uses a browser application program to provide e-mail and newsgroup capabilities.

3. Network Application Management

Networking technologies are expanding the options available for managing the flow of information. We can achieve a collaborative environment for sharing information using web sites and web pages; newsgroups; e-mail; shared folders; and other types of information management automation. For example, networks provide the JTF access to unsecure and secure information, allowing individuals to send and receive unclassified and classified information worldwide. The Nonsecure Internet Protocol Router Network (NIPRNET) provides access to the internet. SIPRNET and JWICS provide access to classified information.

The intranet network infrastructure for a JTF HQ may differ from one JTF to another, but the concepts are generally the same. A JTF intranet is a communications network where access to published information is restricted. The communication standards of the internet and the content standards of the worldwide web (WWW) are normally the basis for a JTF intranet. Therefore, the tools used to create an intranet are normally identical to those used for internet and web applications. Using local area networks (LANs) protected by firewalls is normally the method for establishing a JTF intranet structure.

The JTF IMO must work closely with the JTF web administrator and the component IMOs to develop and establish procedures for network management. The

JTF IMP should identify how the JTF shares information. The JTF IMO must establish procedures enabling each staff section to access, post, and update information. Each staff section ensures the information posted is accurate, current, and relevant.

a. Web Sites and Web Pages.

(1) A well-organized web site assembles vital information, organizes it in a logical sequence, and delivers it efficiently. The JTF HQ, staff directorates, components, and supporting agencies should develop and maintain their own web pages for the site. Information on these web pages should include, but not restricted to, important updates, status reports, common staff products, and current activities.

(2) The JTF should organize the web site around a master "JTF home page." The JTF home page or "front door" sits at the top of the JTF web site acting as a point of entry into the site. In a complex JTF web site, it is impractical to populate the JTF home page with dozens of links. Complicated pages are long and will not load in a timely manner. Therefore, each major element or unit of the JTF should have a mini-home page (major submenu) with direct links back to the JTF home page. JTF mini-home pages are then alternate home pages oriented to specific subgroups of users. Figures III-2 through III-5 depict a hierarchical organizational JTF web site with this type of structure.

(3) Users directly access JTF site pages via a WWW universal reference locator (URL) address. Therefore, the JTF must design the web site so users (at every workstation with a web browser) can quickly navigate regardless of where they enter the site. Ease of navigation, via links from any point on the site is important. All JTF web pages should include a basic set of links logically connecting them to other web pages on the site.

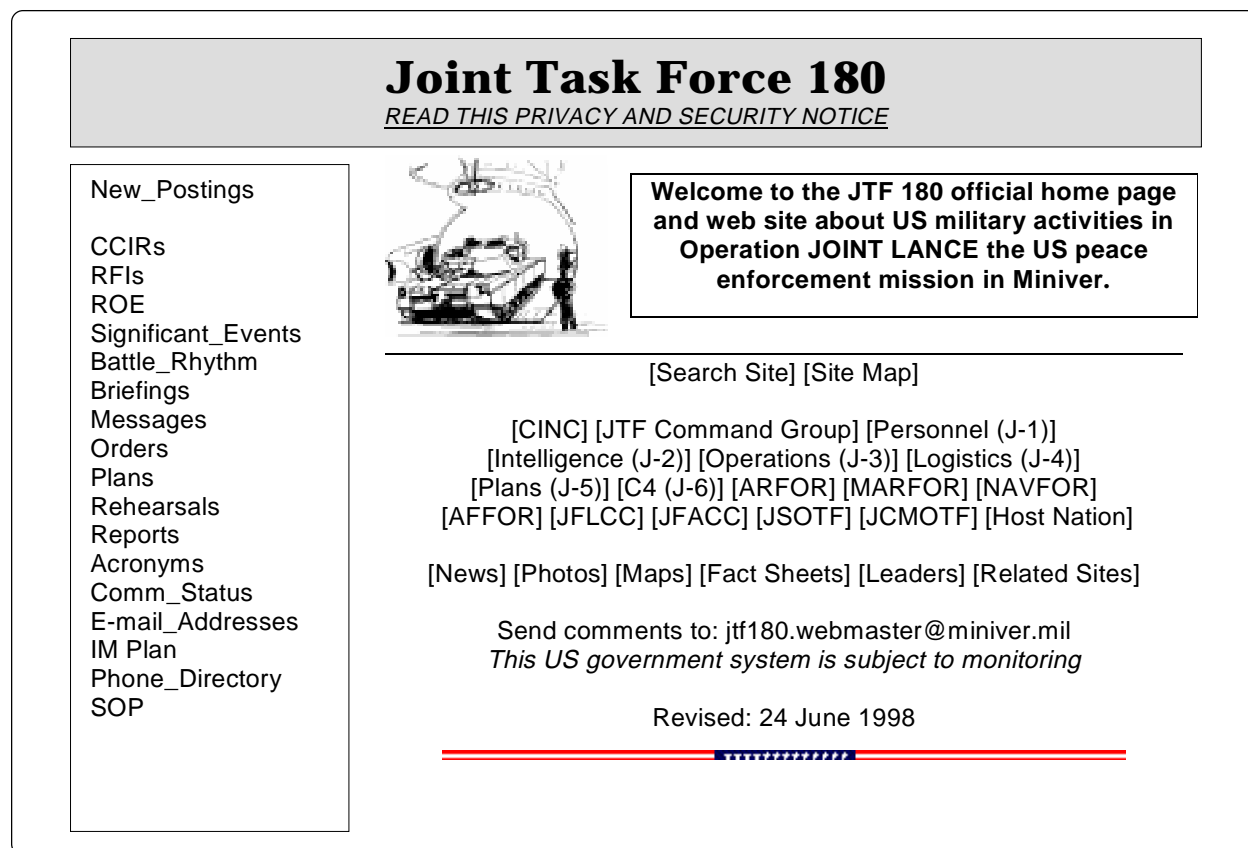


Figure III-2. Sample JTF Home Page

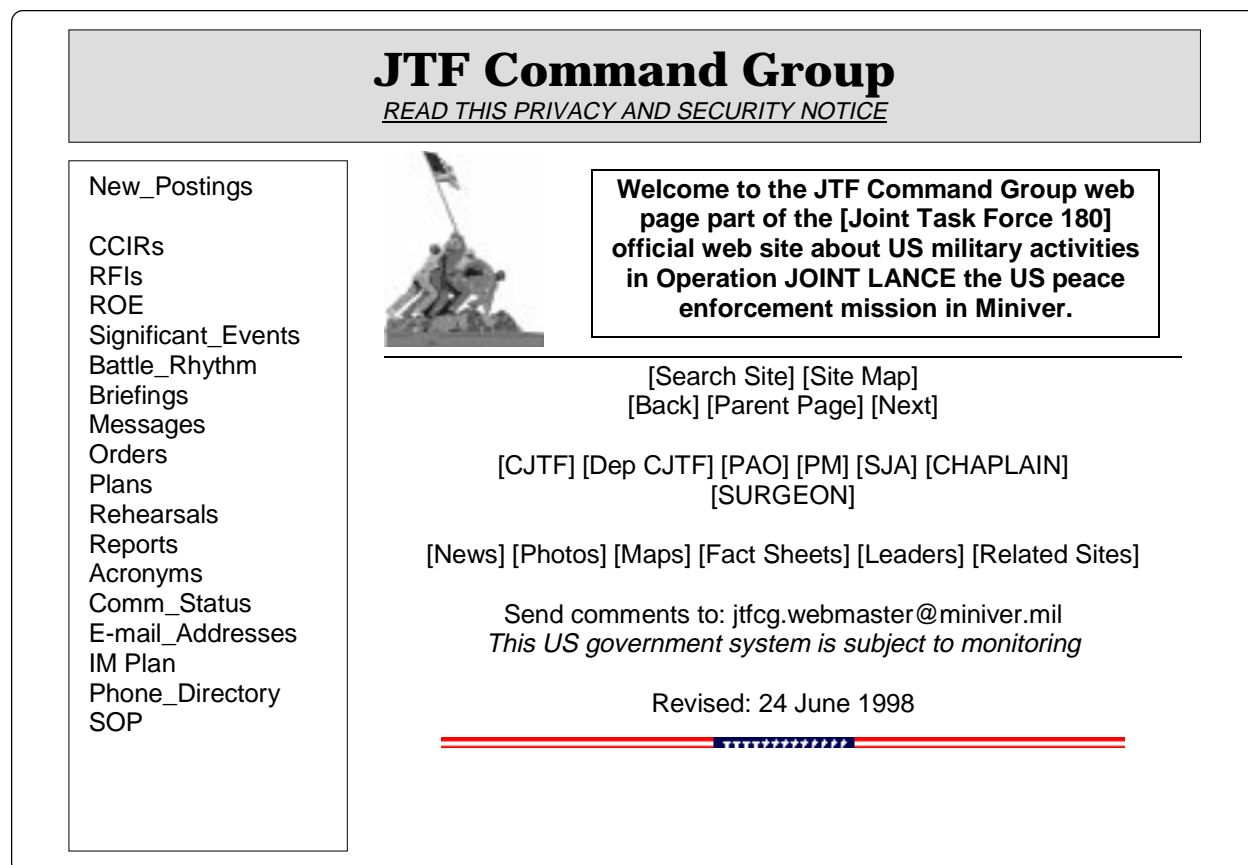


Figure III-3. Sample JTF Command Group Home Page

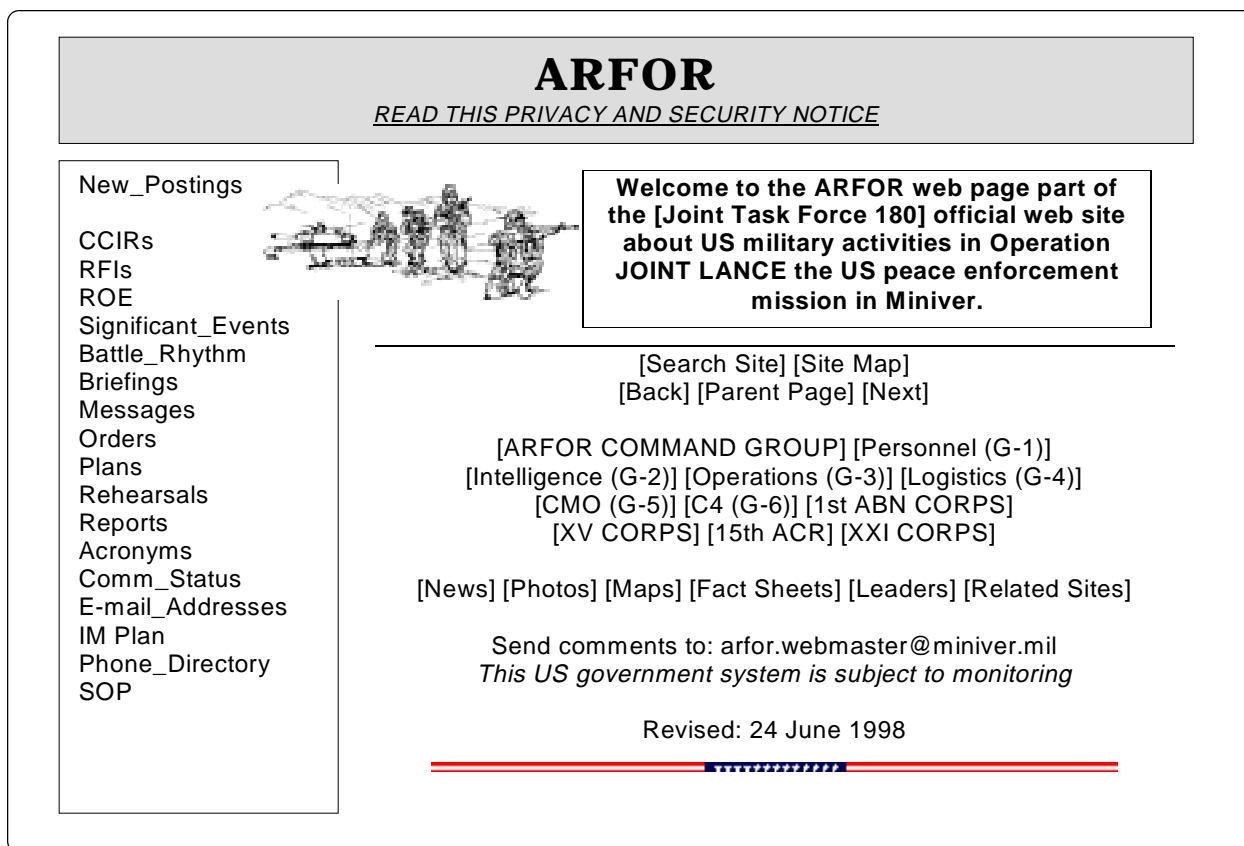


Figure III-4. Sample JTF Component Home Page

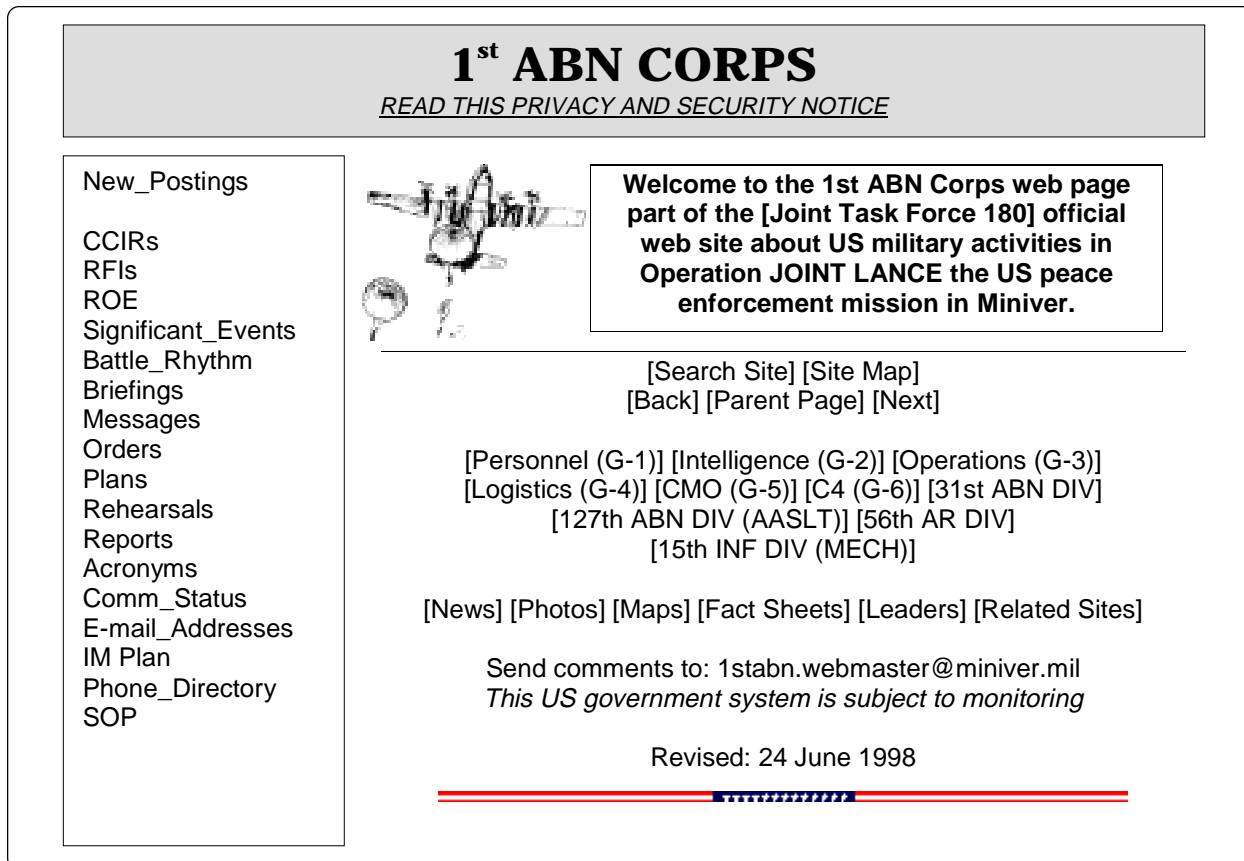


Figure III-5. Sample Major Unit Home Page

b. Newsgroups.

(1) Newsgroups function like electronic bulletin boards and are a means of disseminating information throughout the JTF. Design newsgroups as a network of client servers to obtain the latest news-related information. Running newsgroups from a web browser application allows you to create, post, read, and transfer information. Not all browsers may view newsgroups. You can select a newsgroup, a specific article, follow a given "thread," and transfer files in text format. The information consists of text based files (not binary) transferred via a bulletin board style broadcasting service. Post the files, called "articles," to newsgroups for automatic distribution to sites throughout the intranet.

(2) The design of the JTF newsgroup structure should permit user access to information without burdening them with unneeded information. Newsgroups may be browsed directly or using a hypertext link structure from a newsgroup home page. The hypertext links have the advantage of leading users directly to the information, without having to browse the newsgroups. Table III-2 depicts an example of a JTF newsgroup home page. The newsgroup home page should contain hyperlinks to major category newsgroups.

(3) By selecting hypertext links, the user narrows the information search. In

some cases, establish these links to take the user directly to a desired document. Information available in newsgroups may be orders, rules of engagement (ROE), CCIR, telephone directories, and/or report links. For example, if the user selects J-3 from the JTF newsgroup home page, a new page of links is displayed and contains, but is not limited to, the following:

(a) Staff Instructions. Link to newsgroup containing staff estimates, briefings, reports, guidance, and instructions.

(b) Joint Planning Group (JPG). Link to newsgroup containing mission analysis, courses of action, branch plans, commander's intent, commander's planning guidance, commander's estimate, and decision brief.

(c) JOC. Link to newsgroup containing JTF HQ's significant events log, message board, and master suspense action log.

(4) The JTF J-6 has the overall responsibility of building, maintaining, and modifying newsgroups at the JTF HQ. The component senior communicator is responsible for building newsgroups at component level. Each functional area determines their newsgroup requirements and sends them to their appropriate communicator. Base newsgroup requirements on the type and flow of information

Table III-2. Example JTF Newsgroup Home Page

JTG 176 NEWSGROUP HOME PAGE						
JTF 176 Commander	Command Group	Orders	CCIR	Reports	Phone/E-Mail Directory	Message Board
J-1	J-2	J-3	J-4	J-5	J-6	JPG
AFFOR	ARFOR	MARFOR	NAVFOR	JFACC	JSOTF	JPOTF
JCATF	RFI	ROE	WX	Briefs	INFO MGT	
• Select "INFO MGT" for instructions on how to use newsgroups and to view the JTF 176 Information Management Plan.						

within the JTF. The newsgroup structure depicted in Table III-3 is one example of newsgroup organization. Each staff section monitors their newsgroup ensuring the posting of only appropriate information. The JTF IMO ensures the required topics and procedures are reflected in the JTF IMP. The following protocols apply to newsgroup structure for Table III-3:

(a) Newsgroup. This is the major newsgroup category and is the first hypertext link in the home page newsgroup table.

(b) Subgroup. Refers to minor categories within the newsgroup. These hypertext links lead the user to the desired information in the newsgroup.

Table III-3. JTF Newsgroups

Newsgroup	Subgroup	POC	Purpose
COMMAND GROUP	SJA	SJA	Staff estimates, SJA guidance, briefings, reports
	Surgeon	Surgeon	Staff estimates, surgeon guidance, briefings, reports
	Chaplain	Chaplain	Staff estimates, chaplain guidance, briefings, reports, service schedule
	JIB	PAO	Staff estimates, public affairs guidance, briefings, reports
	Safety	J-1	Safety guidance, instructions
	Security	Security Manager	Security guidance, instructions
	VTC Schedule	Chief of Staff	JTF HQ VTC schedule
	CJTF Schedule	Chief of Staff	CJTF schedule
	DCJTF Schedule	Chief of Staff	DCJTF schedule
	JTF HQ Battle Rhythm	Chief of Staff	JTF HQ schedule
J-1	Staff Instructions	J-1	Staff estimates, briefings, reports, guidance, instructions
J-2	Staff Instructions	J-2	Staff estimates, briefings, reports, guidance, instructions
	INTSUMs	J-2	Intelligence summaries
J-3	Staff Instructions	J-3	Staff estimates, briefings, reports, guidance, instructions
	Operational RFIs	J-3 RFI Manager	All nonintelligence specific
	JOC	JOC	Incoming message board, HQ significant event log, journal, master suspense action log, AUTODIN message board
J-4	Staff Instructions	J-4	Staff estimates, briefings, reports, guidance, instructions, concept of logistics
J-5	Staff Instructions	J-5	Staff estimates, briefing, reports, guidance, instructions, sequel plans, long range plans
J-6	Staff Instructions	J-6	Staff estimates, briefing, reports, guidance, instructions, communications architecture
JPG		J-35/J-5	Mission analysis, courses of action, branch plans, Commander's intent, commander's planning guidance, Commander's estimate, decision briefing
ROE		J-3	Approved rules of engagement
RFI	J-3 RFI	J-3	All nonintelligence related RFIs
	J-2 RFI	J-2	Intelligence related RFIs
CCIR		Chief of Staff	Current commander's critical information requirements
Reports	Reports	Responsible Director	JTF SITREPs, other recurring reports
Orders	Higher HQ Orders	JOC	Orders originating above the JTF
	JTF Orders	JOC	Operations plan, operations order, warning orders, frag orders

Table III-3 JTF Newsgroups (Continued)

Newsgroup	Subgroup	POC	Purpose
ARFOR	Reports	ARFOR	Post JTF required reports
	Supporting Plans		Post JTF required supporting plans
MARFOR	Reports	MARFOR	Post JTF required reports
	Supporting Plans		Post JTF required supporting plans
AFFOR	Reports	AFFOR	Post JTF required reports
	Supporting Plans		Post JTF required supporting plans
NAVFOR	Reports	NAVFOR	Post JTF required reports
	Supporting Plans		Post JTF required supporting plans
JFMCC	Reports	JFMCC	Post JTF required reports
	Supporting Plans		Post JTF required supporting plans
JFACC	Reports	JFACC	Post JTF required reports
	Supporting Plans		Post JTF required supporting plans
JFLCC	Reports	JFLCC	Post JTF required reports
	Supporting Plans		Post JTF required supporting plans
JSOTF	Reports	JSOTF	Post JTF required reports
	Supporting Plans		Post JTF required supporting plans
JPOTF	Reports	JPOTF	Post JTF required reports
	Supporting Plans		Post JTF required supporting plans

(c) Point of Contact (POC). Refers to the proponent directorate or agency responsible for maintaining the newsgroup.

(d) Purpose. A general description of the type of information that may be posted in the newsgroup.

(5) The information transmitted, stored, and posted in a newsgroup directory is the responsibility of the staff element with the newsgroup requirement. The staff element should post and delete information within their newsgroup. Components should use a structure similar to the JTF tailored to their needs. JTF components should coordinate with the JTF J-6 for newsgroup server support.

(6) The JTF should post common information, by topic, to a newsgroup and/or web site. Table III-4 is a sample list of the types of information to include in newsgroups and/or a web site.

c. E-Mail.

(1) E-mail is a highly effective means to communicate information, providing rapid dissemination of time critical information within the JTF. E-mail permits rapid and asynchronous communications,

eliminating “telephone tag.” It permits a single user to communicate with one or several users simultaneously. However to reduce e-mail overloads, consider establishing functional versus individual accounts to avoid unnecessary system stress. This helps prevent a message backlog for personnel not on shift. Additionally, development of a precedence system within e-mail identifies messages requiring timely handling and review.

(2) E-mail can overload the network if used improperly. Unnecessary information and large message attachments stress the system. Use web sites, newsgroups, or public access drives on the LAN to disseminate information. Remove graphics, imagery, and text documents that do not add information content. Develop graphics/briefing slides relying on a minimum of colors since not all users have access to color printers.

(3) At times, it is necessary to notify a large audience that a particular piece of information is available (for example, warning orders). Users should use some discretion in selecting e-mail addressees. In most situations it is preferable to place the information in the appropriate newsgroup then notify intended recipients

Table III-4. JTF Common Relevant Information

CCIRS	Reference Material	Frag Orders
Commander's Intent	DISUM/SITREP	OPLAN
Commander's Additional Guidance	Targeting Plan	Baseline List of Functional Tasks
Casualty Reports Format	Log Requirements	Collection Plan
Phone/e-mail Directory	Commander's Update Briefing	Network/Comm Architecture
BDA	Public Affairs Info	Schedule of Reports
Enemy Organizational Structure	PIR/RFIs	Planning Calendar
Staff Estimates	Commander's Planning Guidance	Weather and Terrain
Mission Analysis	Updated Decision Support Template	ATO
Joint Integrated Prioritized Target List	SOP	High Payoff/High Value

where it may be retrieved, vice attaching the item to multiple e-mail messages. This procedure reduces the bandwidth used when sending multiple copies of e-mails with attachments. Users should periodically review their e-mail group addresses for accuracy and ensuring topic related group members remain interested in the topic. Remember, undeliverable mail may double the system burden (once to attempt delivery and again to notify the sender of the delivery failure). Users should take prompt action to resolve the cause of undeliverable e-mail.

(4) Some e-mail supports information dissemination by providing a notification capability. As the posting authority or sender posts items to newsgroups, they notify users by e-mail.

d. Shared folders are another means to allow access to information. Tables III-5A and III-5B provide examples of shared folders and the information contained in them.

CAUTION

Never assume your intended audience received your article simply because it was posted to a web page or newsgroup. Effective use of web technologies requires establishing a structure allowing for varying degrees of computer literacy, not consuming unnecessary bandwidth, and guiding users directly to the information they seek. Discipline in the posting process and maintenance of the sites is a necessity. Once information has served its useful life cycle, remove it from the web page and/or newsgroup.

e. Other types of information management automation.

(1) Automated Message Handling Systems (AMHSs). This gives the JTF a central location for all types of messages, incoming and outgoing. When you require information on a particular topic, automation is used to sort, filter, and distribute messages. Develop a web front-end to link the web to a particular AMHS. For example, through the use of a commercial e-mail program and the Defense Message Distribution System (DMDS), messages can be automatically passed to designed shared/public folders.

(2) Collaborative Planning Tools. These tools allow input to the process from multiple sources.

(a) Network Meeting Software. White boarding consists of an application allowing two or more computers to link in a way that promotes "real-time" interactive information exchange on-screen between participants.

(b) Internet Relay Chat (IRC). IRC is an interactive conferencing tool on GCCS, allowing users to open "chat channels" similar to conference calling via on-screen exchange. Chat channels permit one-to-one or one-to-many communications. Intended topics of discussion generally define communications channels. Typical IRC channels may be established for time-phased force and deployment data (TPFDD) developers and validators, information managers, etc.

Table III-5A. JTF Shared Message Folders

J-1	J-2	J-3	J-4	J-5	J-6
Admin	Action Items	Air Ops	Briefings	Briefs and Slides	Admin
Completed Taskers	Admin	Airlift	General Info	Force Protection	Directories/Rosters
Daily News Briefs	JULLS	Fighters	RFI	J-1	Organization Structure
Incoming Messages	MSG-Air	Army Aviation	Play-Info	J-2	Briefing Slides
Need Information Requests	MSG-BDA	Army Ground	Reports	J-3	Incoming Messages -COMSTAT -SITREP
Outgoing Messages	MSG-Force Protection	CMOC	Admin	J-4	Outgoing -COMSTAT
Personnel	MSG-Ground	Everybody Read	Civil Engineers	J-5 Staff	MSEL -Incoming -Responses
SITREPS	MSG-IIR	EWO	Comptroller	Media	JULLS
J-1 Reports	MSG-INSUM	General Info	Contracting	Taskers	Admin
Personnel Status Request	MSG-Naval	Info Ops	Director	RFI	Computer System Support
Receipts (Verification)	MSG-Political	JOC	Fuels		Current Ops
Policy Guidance	MSG-Refugees/Med	JULLS	LNO		FRAG Management
Postal	MSG-SITREPS	LNOs (J-1, J-2, J-3, J-4, J-5, J-6)	Medical		Future Ops
Incoming	MSG-Targets	MSEL Events	Plans		Future Plans
Outgoing	MSG-Terrorist Activity	Navy Ops	Services		J-6
Suspenses	MSG-Warning/Execute Order	Ops/Plans	Supply		JCCC
	WMD/NBC/SCUDs	Ops-Analysis	Suspenses		Joint Key Management
		FRAGOS	Transportation		JULLS
		Warning Orders	Weapons		LNO (DISA)
		PSYOP	JULLS Inputs		Networks
		RECCE	Maintenance		Policy Guidance
		SITREP Inputs			Refugee Evacuation Procedures
		SOF			SITREP Inputs
		Special Staff			
		JOPEs			
		Space			
		Taskers			
		TMD			
		Weather			

Table III-5B. JTF Shared Message Folders

JTF Message Center Folders	Chief of Staff Admin Public Folders
Incoming e-mails	Alert roster
Incoming messages	Continuity
Incoming RFIs	Chief of staff organization (chain of command/responsibilities)
	Chief of staff policy directives
Outgoing e-mails	
Outgoing messages	Note: Paper read files are produced.
Outgoing RFIs	
Message center policies	
Temporary e-mails	

4. LAN

The JTF LAN can be set up with shared and/or private hard drive space. Private drive space is intended to limit access to stored data. Access is generally limited to specific functional areas, as defined by user login names (that is, specific joint-code staff sections). The shared or “public” drives are accessible by anyone given access by the LAN administrator. The public drives organized with appropriate subdirectories, increase staff visibility of files and provide the opportunity for a larger staff audience (at one location) to coordinate, review, and approve staff issues. The LAN administrator establishes the shared drives. Staff sections are responsible for the currency, accuracy, and maintenance of their shared drive information.

5. AUTODIN Message Communications

AUTODIN messages are the approved means for record traffic. The JTF J-6 should publish an associated plain language address (PLA) directory for the JTF staff, components, and supporting organizations.

The message center, operating on a 24-hour schedule, transmits outgoing messages. Each directorate, to prevent unauthorized transmission or reception of record traffic, should establish formal message release and receipt authority.

6. VTC

a. Improvements in digital video compression and readily available high-capacity transmission systems make it possible for secure, interactive color video worldwide. The primary purpose of the JTF VTC capability is support of the JTF commander. The secondary purpose of the JTF VTC capability is to facilitate the transfer of information between subordinate commanders and staffs. While VTC is quickly becoming the system of choice, the JTF commander could use alternate methods of communication such as conference calls if a VTC system is not available. VTC provides—

(1) Verbal and visual communications on the same medium.

(2) Communications medium to readily identify who is speaking.

(3) Visual communications signals (body language, etc.) missing with other forms of electronic communications.

(4) An alternate means of communications when other means are not available.

(5) Interactive information exchange between two or more elements.

b. Types of JTF VTCs.

(1) General Service (message) [GENSER]. This is the primary means of VTC between components and the JTF HQ for UNCLASSIFIED and up to TOP SECRET (TS) Collateral.

(2) JWICS. JWICS VTC is the primary means of VTC involving SCI requirements.

c. VTC Concept. The GENSER and JWICS VTCs should be available for scheduling 24 hours a day except for required maintenance. The JTF battle rhythm dictates the schedule of the VTCs, and the JTF HQ is network control for the VTC. The JWICS VTC is the backup for the GENSER VTC. The JWICS VTC is always located within a permanent sensitive compartmented information facility (SCIF) or a tactical SCIF (T-SCIF).

d. VTC Procedures.

(1) GENSER VTC. Scheduling of the GENSER VTC is the responsibility of the JTF chief of staff. The VTC scheduling officer works closely with the JTF IMO in developing the VTC schedule. The JTF commander is the primary and priority user of this system. Components, staff directorates, and supporting agencies desiring to schedule a GENSER VTC submit their requests to the VTC scheduling officer. Prior coordination with the controlling SSO is mandatory for access to the JWICS VTS suite, especially for

JWICS VTC participation by persons *not* indoctrinated for SCI. Coordination should include clearance and access verification for all participants who do not have routine access to the SCIF. The VTC scheduling officer should post the schedule at the location determined by the IMO and contained in the IMP. Prioritization for usage of the GENSER VTC shall be in the following order, except as designated by the JTF chief of staff:

(a) CJTF-directed VTCs.

(b) Scheduled JTF VTCs.

(c) CJTF and component commander requested VTCs (for example, commander to LNOs or other component commander).

(d) JTF HQ staff requested VTCs.

(e) Other requested VTCs.

(2) JWICS VTC. Scheduling is the responsibility of the JTF HQ, JISE director. JWICS VTC use is coordinated through the JISE Director. Prioritization should be the same as for the GENSER VTC. The JTF chief of staff adjudicates scheduling disputes.

e. Visual Aids. Visual aids are encouraged for VTCs. However, they must be concise and readable to the viewer. Make every effort to provide advance copies of visual aids to all commands participating in the VTC before the VTC. Guidelines for visual aids on GENSER and JWICS VTC follow:

(1) Use sentence case (upper and lower case) for text on slides.

(2) Use no smaller than 28-point courier font text for text on slides.

(3) Use pure black and white, when possible, for contrast and ease of reading.

(4) Keep graphics simple.

(5) Mark the classification of visual aids appropriately.

(6) Attempt to display no more than 7 lines of text per slide.

(7) Date each brief following presentation.

f. Security. Because of the range of security classifications potentially passed during the VTCs, each location must ensure that personnel with appropriate clearance and access attend the VTCs.

7. Global Broadcasting System (GBS)

GBS provides receive-only high-speed flow of high volume data to units in garrison, deployed, or moving. It supports existing CINC requirements by providing the capability to distribute large information products to deployed user platforms. Develop and distribute information products using a “Smart Push and/or User Pull” philosophy to avert saturating deployed forces with information overload. The major operational elements of GBS are pertinent to IM:

a. Users. Users are deployed warfighters in the CINC’s area of responsibility (AOR). GBS is to be transparent as possible while servicing the needs of the users with required information products.

b. Information Producers. Information producers can be just about anything that produces a product the warfighter wants.

c. Information Dissemination Management (IDM). IDM provides the right information to the right place at the right time in accordance with commander’s policies and optimizing the use of information infrastructure resources. It involves the safeguarding, compilation, cataloguing, storage, distribution, and retrieval of data; manages the information flow to users; and enables the execution of the commander’s information policy.

d. Theater Information Management (TIM). The role of TIM is establishing the

CINC's policies and procedures for information flow. TIM accomplishes six functions:

- (1) Directs GBS operation.
 - (2) Coordinates broadcast schedule.
 - (3) Manages apportioned resources.
 - (4) Identifies new products.
 - (5) Reviews and validates user profile databases.
 - (6) Audits user pull.
- e. Satellite Broadcast Management. Satellite broadcast management executes the GBS broadcast by fulfilling eight basic functions:
- (1) Builds a schedule and program guide.
 - (2) Coordinates information products.
 - (3) Conducts traffic analysis.
 - (4) Constructs and transmits the broadcast stream.
 - (5) Provides for protection of data.
 - (6) Controls the GBS broadcast technically.
 - (7) Controls remote enabling/disabling of receive suites.
 - (8) Establishes and maintains the user profile database.

8. Priority of Communication Means

The JTF J-6 establishes specific responsibilities for establishing connectivity between the JTF HQ and components. Normally, the higher HQ is responsible for establishing all connections to lower HQ. The JTF should possess redundant means of voice communications, data transfer, and functional specific data

systems. The following is a prioritized listing of communication means normally found within the JTF:

- a. Voice Communications—Defense Switched Network (DSN).
 - (1) Commercial secure telephone unit III (STU-III) phones.
 - (2) KY68 tactical lines.
- b. Radio Communications Network.
 - (1) JTF command net.
 - (2) Intelligence net.
 - (3) Air coordination net.
 - (4) Theater missile defense net.
- c. Data Transfer.
 - (1) SIPRNET/NIPRNET.
 - (a) Home page.
 - (b) E-mail.
 - (c) Newsgroups.
 - (2) AUTODIN.
 - (3) Facsimile.
 - (4) STU-III file transfer.
- d. Functional Specific Communications.
 - (1) SCI intelligence collection-JWICS.
 - (2) STU III dial-in.

The joint force must have information to operate. This information should be relevant, essential, timely, and in a form that warriors understand and can use to act

Joint Publication 6-0

INFORMATION MANAGEMENT REQUIREMENTS, PROCESSES, AND PROCEDURES

*...not just more information faster but
better and more useful information...*

JFQ Winter 1996-97

1. Background

All leaders depend upon information to plan and execute missions. This chapter focuses on the processes for obtaining and disseminating information within the JTF.

2. CCIR

a. The CJTF has specific information requirements, directly affecting decisions and successful execution of operations. Using CCIR focus the staff on the information the commander requires and feels is critical. This enhances the staff's ability to integrate (filter) information and remain focused on the information of the highest value. CCIR may change as events unfold. Therefore, CCIR require continuous assessment for relevance to current and future situations.

b. The following are some techniques for CCIR development and management:

(1) Review CCIR for each operation, branch, and sequel plan. During the planning process, staff directors may propose CCIR to the JPG. The JPG chief consolidates the proposed CCIR for CJTF consideration and approval. After approval, the JOC posts the CCIR in an electronic medium (for example, newsgroup-CCIR, home page, etc.). In some instances, the CJTF's guidance on CCIR could lead to operation, branch, or sequel plans.

(2) During the conduct of operations, review the CCIR continuously for relevancy. Review, modify, or archive the CCIR during the CJTF daily update briefing. The JTF staff should submit recommended changes to CCIR to the J-3. The J-3 reviews and compiles the recommended changes for presentation to the CJTF for approval.

(3) All members of the JTF are responsible for reporting information that may satisfy CCIR. However, each staff director should ensure processes within their directorate are in place to filter and fuse raw data before submission. CCIR tracking/monitoring is the primary task of the JOC. When a CCIR is met or there are indicators that one is about to be met, the JOC makes an immediate "voice" report to the CJTF, deputy commander, joint task force (DCJTF), principal staff directors, and component operations centers. Voice reports are followed by Flash messages via GCCS and e-mail to all staff directors and component commanders. When CCIR are obtained, the JOC/JISE analyses the implications on current and future plans, then briefs the CJTF. This analysis should include any recommendations for modifications to CCIR or additional CCIR.

3. RFI

a. The JTF HQ establishes RFI procedures to provide a systematic method for requestors to obtain information. Joint Publication 1-02 defines the term "RFI" as—*Any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing*

requirements or scheduled intelligence production. A request for information can be initiated to respond to operational requirements and will be validated in accordance with the theater command's procedures.

b. The J-2 processes intelligence related RFIs and the J-3 all other RFIs. The J-2 and J-3 assign an RFI manager to receive and prioritize RFIs. A tracking system known as the COLISEUM is established to register, validate, track, and manage crises and noncrises intelligence information requirements. COLISEUM functions as an application on the JDISS workstation providing connectivity and interoperability with other intelligence systems supporting operational users.

c. Send RFIs to higher, subordinate, adjacent HQ or to other agencies requesting the information necessary to support the planning and decisionmaking process (see Figure IV-1). Effective RFI procedures provide the JTF an “information pull” mechanism providing requestors access to a variety of vital information. RFI procedures do not replace normal staff coordination or substitute for researching information using other means (for example, intelligence link via the SIPRNET and NIPRNET) available to JTF members. Instead, the RFI process provides a mechanism for a formal request to higher echelons when the issue or question is beyond the resources of the staff. In addition, the process provides visibility of those requests forwarded, their status, and responses to these requests.

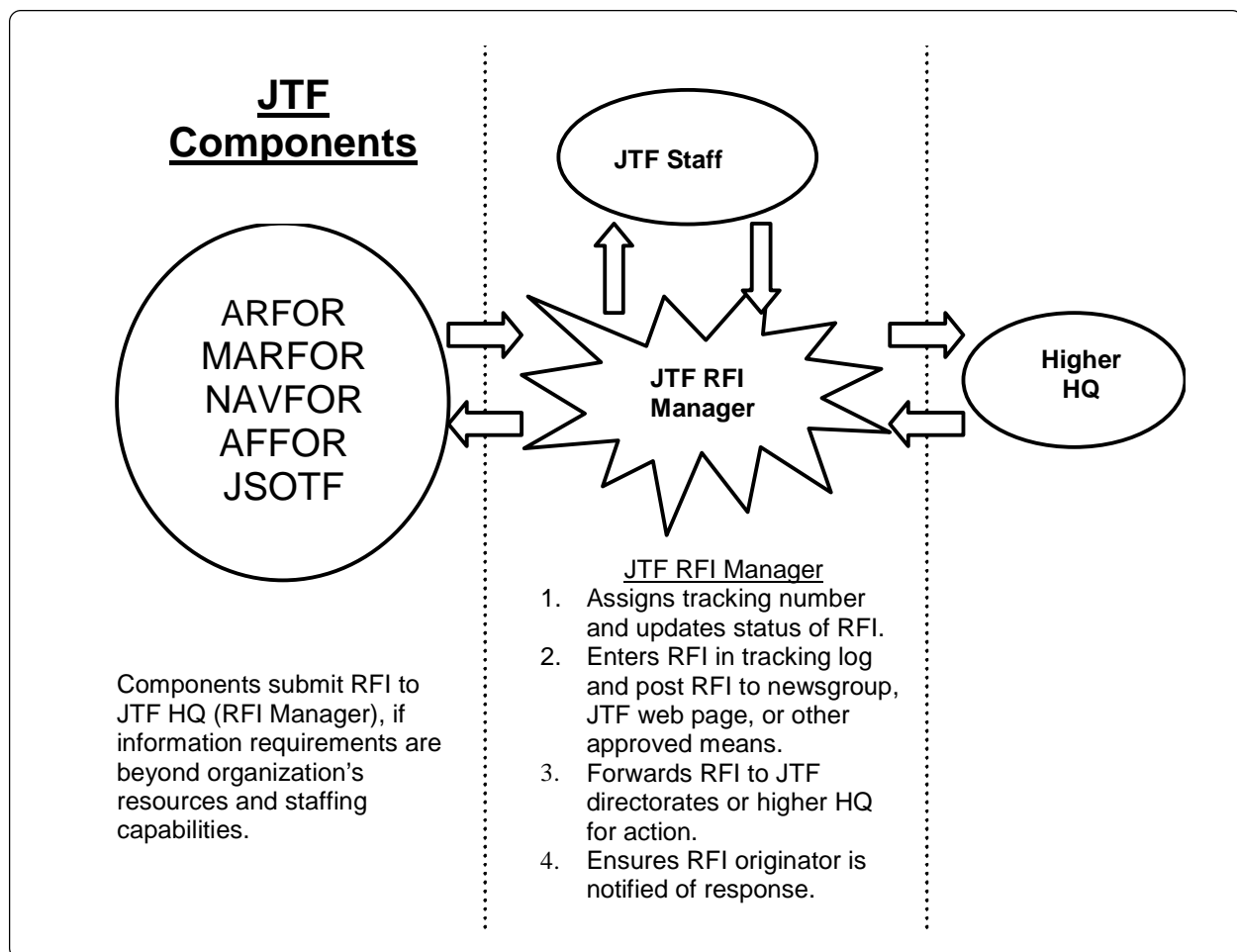


Figure IV-1. Request for Information Flow Chart

d. Components submit RFIs to the JTF HQ that are beyond their capability and staff resources to answer. Components submit intelligence related RFIs to the JTF J-2 RFI manager via COLISEUM, SIPRNET, e-mail/web pages, or other approved means in accordance with established procedures. The JTF J-2 RFI manager assigns an internal RFI tracking number only if not using COLISEUM for J-2 RFI management. Components submit operational related RFIs to the JTF operations RFI manager (J-3/J-5), via SIPRNET e-mail/web pages or other approved means. The JTF operations RFI manager assigns an internal RFI tracking number, forwards it to the appropriate JTF staff directorate for action, then posts RFI responses to newsgroups, JTF web pages, or other approved means. If the JTF staff is unable to provide an answer, the JTF operations RFI manager forwards the RFI to higher HQ for resolution.

e. The JTF staff directorate RFI manager submits RFIs to the JTF RFI manager by posting it to a newsgroup, JTF web page, or other approved means. The JTF RFI manager processes the request and forwards it to the appropriate agency for resolution. Each directorate is responsible for monitoring their RFIs and closing the request.

f. RFI Guidelines.

(1) Limit RFI to one question per request. (Multiple questions increase response time.)

(2) State RFI as a specific question and provide sufficient detail so the request is completely understood.

(3) Resubmit the RFI with additional comments or clarification, if a RFI is not completely answered.

(4) Submit a new RFI if additional information is required.

(5) Submit intelligence RFIs through the intelligence RFI system (COLISEUM).

(6) Spell out acronyms the first time they are used.

(7) Pass staff action RFIs to appropriate staff section.

(8) Obtain approval from the chief of staff for the specific format for RFIs.

(9) Include the following information in RFI request:

(a) Classification.

(b) Priority. (Routine, Priority, Immediate, or Flash).

(c) Time/Date.

(d) Required not later than (NLT).

(e) Requestor.

(f) To (who should answer).

(g) Subject.

(h) Amplifying Data (question).

(i) Recommended method of transmission.

(10) Intelligence related RFI requests include—

(a) Narrative description.

(b) Justification.

(c) Sources consulted.

(d) Date desired.

(e) Latest time information of value (LTIOV).

(f) Classification of response (desired class and accepted class).

(g) Remarks (any additional information not included in the narrative).

(h) POCs (include both the JTF RFI manager as well as the requestor).

g. The RFI tracking log (Table IV-1) is a simple tool for use in newsgroups, web pages, or other electronic medium. The purpose of this log is providing JTF-wide visibility of the submitted RFIs and the status of responses. The status column of the request log is color-coded as follows:

(1) Red indicates a pending request.

(2) Amber indicates a response awaiting requestor's review. The requestor of an RFI closes all "amber" coded RFIs if the response answers the RFI completely by changing the status indicator to green.

(3) Green indicates that the RFI has been answered and that action is complete.

4. CTP Management

a. The JTF CTP feeds the CINC's COP as identified in the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3151.1, *Global Command and Control System Common Operational Picture Reporting Requirement*. This instruction identifies specific reporting, training requirements, and responsibilities for the COP/CTP management. A JTF CTP requires effective and efficient management procedures. Some of the data feeds into the CTP are automatic, while some are manual. Effective management of the CTP prevents

the display of outdated or unwanted surface, air, or subsurface locations/tracks in a particular map view.

b. The JTF CTPM coordinates the actions required to synchronize management between the JTF components and the JTF HQ. The CTPM should ensure that the procedures identified in CJCSM 6120.01A are followed for track/location management on tactical data links between Service/functional components and subordinate echelons. The CTP requires the following inputs:

(1) Blue air, maritime, and ground force tracks/locations.

(2) Red air, maritime, and ground tracks/locations.

(3) White/neutral/unknown air, ground, and maritime tracks/locations.

(4) Operational overlays.

(5) Intelligence overlays.

(6) National Imagery and Mapping Agency (NIMA) products.

5. Collaborative (Integrated) Planning System (CPS)

The CPS is a compilation of systems; software applications; and tools designed to support JTF planning, decisionmaking, execution, and assessment. The JTF CPS should allow input by multiple personnel both at the JTF and at remote locations. Products derived and utilized by the distributed CPS should be compatible and interoperable with those used by the CINC. The JTF CPS should—

Table IV-1. RFI Tracking Log

TRACK #	TIME/DATE SUBMITTED	PRIORITY	REQUIRED NLT	SUBJECT	REQUESTOR	STATUS
1						
2						
3						

a. Include an interactive visual projection capability so members of the JTF can see the collaborative effort both on their workstation screen and on a large "movie screen" display.

b. Support the JTF planning process in a series of logical steps and provide an explanation or "how to" section.

c. Provide products in the correct format so that a CJTF's briefing is presented right off the working screens.

d. Be capable of scanning documents into required databases so all JTF components can view higher, adjacent, and supporting command orders and messages.

e. Include databases that can be accessed to include access to force lists and availability, intelligence feed, TPFDD data, worldwide map system, unit capabilities, equipment, organization for each Service (US), and other country forces as required.

f. Include an analysis capability to wargame various courses of action, branch plans, and/or sequels. Possess the ability to alert and recognize information tethered to CCIR. Contain a COA selection tool to assist planners in performing the analysis involved in COA selection.

g. Possess the capability to print information and overlays contained in the system. Possess the ability to print laminated overlays to the scale of the maps utilized.

h. Possess the capability to portray maps with operational graphics (for example, boundaries, fire support coordinating measures, friendly and threat units, decision support templates, collection plans, fire support plans, and barrier plans, etc.).

i. Have the capability to transfer information from working/briefing formats to a message format to generate messages

without having to build the messages from scratch.

6. Joint Operations Center/Joint Intelligence Support Element Assessment Cell (JAC)

During operations, massive amounts of data flow into the JOC from a myriad of sources. The personnel assigned to the JOC/JISE must filter, sort, and turn data into information. That information must be fused, analyzed, and converted into knowledge. The information is then submitted up the chain of command so the staff can make appropriate recommendations concerning JTF operations. The CJTF ultimately uses these recommendations to make informed decisions. It is essential this assessment process be thorough, accurate, complete, and conducted by individuals qualified and experienced enough to achieve that end state. One optional technique is forming a JAC to conduct this analysis.

a. Purpose. The JAC fuses enemy/friendly intelligence and operational information. After thorough analysis, the JAC provides results of the assessment with recommendations to the J-3. The JAC tracks and analyzes all approved CCIR. After review, the JAC recommends the addition of new or archiving of existing CCIR to the J-3 and coordinates the accurate posting of all current, approved CCIR in the JOC.

b. Reporting and Coordination. The JAC reports directly to the J-3 and J-2. If the staff principals are not available, it reports to the deputy JOC chief. The JAC coordinates with the JISE chief as required. The JAC receives primary information from the current operations/current intelligence cells.

c. Function. The JAC's function is maintaining operational awareness of the battle space by the constant fusion and assessment of all friendly and enemy information. *(The JAC has no tasking*

authority over the watchstanders in the JOC. It is incumbent on the J-3 to ensure that the JAC receives all required information to accomplish its mission.) The JAC must keep the J-3 informed; it must answer the questions of “what is our situation—what is the enemy’s situation—what does it mean to our operations?” The JAC’s mission is critical to the success of the JTF mission. Accordingly, the J-3 must ensure the JAC’s role is *isolated to its mission and function only*.

d. **Organization.** The following organization is one recommended solution for staffing the JAC. Each JTF must evaluate its mission, then establish the manning level and required personnel specialties for the JAC. Each shift of the JAC should be comprised of 6 individuals, each with a specific warfare specialty. JAC personnel must have service experience, qualification, and subject matter expertise. They should have a broad enough background to grasp the concepts required to fuse and analyze joint operations. Joint warfighting or joint staff experience is a plus. The senior officer assigned in the JAC is designated the JAC chief. The billets within the JAC are as follows:

- (1) Ground combat officer (0-5).
- (2) Naval officer (0-5).
- (3) Tactical aircrew Air Force officer (0-5).
- (4) Intelligence officer (0-5).
- (5) Special operations officer (0-5).
- (6) Administrative/technical support (E-5 to E-7).

e. **Intelligence/Operations Fusion.** Review both the enemy and friendly situations to conduct a complete and thorough assessment. The current operations cell reports friendly information to the JAC. The current intelligence cell

reports enemy information to the JAC. Both cells continuously report confirmed, accurate, filtered, processed, and categorized information to the JAC. Subsequent “subanalysis” fuses this information with friendly information for each appropriate warfare area. Reanalyze these warfare area “subanalyses” in *aggregate*—only then is a complete, thorough assessment derived and accurate situational awareness achieved.

7. JTF Daily Operations Cycle (Battle Rhythm)

JTF information requirements are often predictable. The JTF HQ staff can position information at its anticipated points of need to speed information flow and reduce demands on communications systems. One method is establishing a daily operations cycle for briefings, meetings, report requirements, etc. (Table IV-2 depicts an example).

The “daily operations cycle” is synonymous with “battle rhythm.” To ensure information is available when and where required, the JTF daily operations cycle is essential. All JTF staff, components, and supporting agencies should participate in the development of the daily operations cycle. The JTF chief of staff should be the approval authority for changes. When establishing the daily operations cycle, the JTF HQ should—

- a. Monitor the daily operations requirements of higher HQ.
- b. Ensure all subordinate daily operations cycles meet the needs of the JTF.
- c. Monitor for conflicting JTF requirements (particularly for key personnel).
- d. Keep changes to a minimum.

Table IV-2. Sample JTF HQ Daily Operations Cycle

Local	ZULU	Event
0900	1400	Shift change CJTF VTC with components
1000	1500	JFACC VTC
1100	1600	JOC/JISE update
1200	1700	Plans synchronization meeting
1300	1800	J-2 VTC with components press conference
1400	1900	Future plans update to CJTF
1500	2000	J-3 staff meeting
1600	2100	JPG plans synchronization meeting
1700	2200	Component SITREP due JTF J-3
1800	2300	J-1 VTC with components
1900	0000	JOC shift change and update brief
2000	0100	SITREP transmitted
2100	0200	Shift change brief JFACC VTC
2200	0300	JTF SITREP due to CINC CJTF JAC update
2300	0400	Chief of staff update
0000	0500	Public affairs update
0100	0600	Plans synchronization meeting
0200	0700	J-2 VTC with components
0300	0800	ROE/force protection meeting
0400	0900	J-3 VTC
0500	1000	CJTF staff brief
0600	1100	CJTF call with CINC
0700	1200	JTCB meeting
0800	1300	J-4 VTC with components

8. Reports Development

Table IV-3 contains some sample reports, requests, and orders for which the JTF and components may be responsible. Refer to Joint Publication 1-03, *Joint Reporting Structure (JRS) General Instructions*, Chapter V, for a summary of each report. The table provides a brief description of the report, sender, receiver, when and how to transmit, and whether it is in US Message Text Format (USMTF). This matrix organizes reports according to the responsible directorate. The matrix reflects the following information:

a. Report Type. Report title or type of information provided.

b. Submitted By. The component or agency normally responsible for submitting the report to the JTF.

c. As of Time. Close out time for recurring reports, not applicable (N/A) for nonrecurring reports.

d. Posted NLT. Time to post the report for JTF review.

e. Where Posted. The newsgroup or web page location to post the report.

f. Notify. Whom to notify after posting the report. Normally not required for recurring reports.

g. Notification. Preferred method of notifying JTF following posting.

h. Precedence. The precedence to use when notifying the JTF the report is available (not applicable to some notification methods).

Table IV-3. JTF Reports Matrix (1 of 3)

Report Title	Submitted By	Submit As Of	Arrive NLT	Transmission Type	Precedence	Addressee	Info To
Personnel Status Report	Components	1500	2100	E-mail home page	Routine	JTF J-1	
Casualty Spot Report	Components	As required	As required	E-mail	Routine	JTF J-1	
EPW/CI/DET Report	Components	1800	2400	E-mail	Routine	PM	JTF J-2
Intel Requests for Information (RFI)	Components	As required	As required	COLISEUM	Priority	JTF J-2	
Captured Materiel Report	Components	As required	As required	E-mail	Priority	JTF J-2	
Component INTSUM	Components	0400/1600	1800/0600	JDISS	Routine	JTF J-2	Components
Spot Reports	Components	As required	As required	E-mail	Routine	JTF J-2	
JTF Recon 2	JTF 2	As required	As required	AUTODIN JDISS	Priority	CINC	Components
Component Recon 3	Components	As required	As required	AUTODIN JDISS	Priority	JTF J-2	CINC
Component Recon 4	Components	As required	As required	AUTODIN JDISS	Priority	JTF J-2	CINC
JTF DISUM	JTF J-2	2200		AUTODIN Home page	Routine	CINC	Components
JTF Graphic Supplement	JTF J-2	1000/2200		Home page	Routine	CINC	Components
Component INTSUM w/ Graphic Supplement	Component J-2	0800/2000		Home page JDISS	Routine	JTF J-2	
Collection Emphasis Message	Component J-2	Last 24 hrs		AUTODIN Home page	Routine	JTF J-2	
JTF Collection Emphasis Message	JTF J-2	Last 24 hrs		AUTODIN Home page	Routine	CINC	Components
SITREP (CDRs Situation Report)	Components	2400	0200	AUTODIN Home page	Priority	CJTF, J-3	Components
JTF CDR SITREP	JTF J-3	1000/2000	1000/2000	AUTODIN Home page	Priority	CINC	Components
Orders (FRAGO, WARNORD, OPORD)	JTF J-3	As required	As required	AUTODIN Home page	Priority	All	Components
RFIs (except intel)	Components	As required	As required	E-mail	Priority	JTF RFI manager	
RFIs (except intel)	JTF RFI manager	As required	As required	Home page	Priority	CINC	
Engagement Status	Components	As required	As required	E-mail	Priority	JTF J-3 ADA	Components

Table IV-3. JTF Reports Matrix (2 of 3)

Report Title	Submitted By	Submit As Of	Arrive NLT	Transmission Type	Precedence	Addressee	Info To
SAM Report	Components	As required	As required	E-mail	Priority	JTF J-3 ADA	Components
Significant Event Spot Report	Components	As required	As required	E-mail	Priority	JTF J-3 ADA	Components
Daily Targeting Guidance MSG	JTF J-3	1200	1300	Home page	Priority	Components	JTF Staff LNOs
Target Report	Components	Continuous	Continuous	E-mail	Priority	JFACC JIC	JTF J-3
Target Bulletin	J-3	Continuous	Continuous	E-mail	Priority	Components	CINC
Daily PSYOP Report	Components	2400	0200	E-mail	Priority	JPOTF/J-3	Components
PSYOP Spot Report	Components	As required	As required	E-mail	Priority	JPOTF/J-3	Components
NBC 1	Components	As required	As required	Voice, E-mail	Flash	JTF NBC	Components
NBC 2	Components	NLT 2 hours after "as of time"	As required	GCCS E-mail	Immediate	JTF NBC	Components
NBC 3	Components	As required	As required	GCCS E-mail	Immediate	JTF NBC	Components
NBC 4	Components	As required	As required	GCCS E-mail	Immediate	JTF NBC	Components
NBC 5	Components	After survey completed	As required	GCCS E-mail	Immediate	JTF NBC	Components
NBC 6	Components	When requested	When requested	GCCS E-mail	Immediate	JTF NBC	Components
LOGSITREP	Components	0600-0600	1000	Home page	Routine	JTF J-4	
LOGSITREP	JTF J-4	0600-0600	1800	Home page	Routine	CINC	Components
Munitions Report	Components	0600-0600	1000	Home page	Routine	JTF J-4	
Bulk Petroleum Contingency	Components	0600-0600	1000	Home page	Routine	JTF J-4	
Munitions Report	JTF J-4	0600-0600	1800	Home page	Routine	CINC	Components
Bulk Petroleum Contingency	JTF J-4	0600-0600	1800	Home page	Routine	CINC	Components
Environmental Status	ARFOR	Weekly		Home page	Routine	J-4	
Engineer SITREP	Components	2400/0800	0200	Home page	Routine	J-4	
Engineer Compatible Report	Components	As required	As required	Home page	Routine	J-4	
Civil Affairs Daily Report	Components	2400	0600	E-mail	Routine	JCMOTF	Components
Civil Affairs Spot Report	Components	As required	As required	E-mail	Priority	JCMOTF	Components

Table IV-3. JTF Reports Matrix (3 of 3)

Report Title	Submitted By	Submit As Of	Arrive NLT	Transmission Type	Precedence	Addressee	Info To
CA Resource Report	Components	2400	0600	E-mail	Routine	JCMOTF	Components
Civil Affairs Report	Components	2400	0800	E-mail	Routine	JCMOTF	Components
Dislocated Civilian Report	Components	2400	0600	AUTODIN Home page	Routine	JCMOTF	Components
Legal Report	Components	2400	0400	AUTODIN	Routine	JTF SJA	Components
Public Affairs Report	Components	1800	2000	AUTODIN Home page	Routine	JIB JTF PAO	
Religious Ministry Spot Report	Components	1200	1800	E-mail	Routine	JTF chaplain	
Medical Spot Report	Components	As required	As required	GCCS E-mail	Priority	JTF surgeon	
Medical Status Report	Ech III med fac	2359	0400	GCCS E-mail	Routine	JTF surgeon	JTF J-4
Medical Survey	Ech III med fac	Weekly		GCCS E-mail	Routine	JTF surgeon	JTF J-4
Blood Report	Blood unit	2359	0600	GCCS E-mail	Routine	JTF surgeon	JTF J-4
Medical Supply Status	SIMLM	2359	0600	GCCS E-mail	Routine	JTF surgeon	JTF J-4
Medical Regulation	Ech III med fac	As required	As required	GCCS E-mail	Priority	JMRO	JTF J-4
Air Evac Request	Air evac request	As required	As required	HF secure	Priority	AECC	
Air Evac Response	Air evac response	As required	As required	HF secure	Priority	AELT	
Air Evac Confirmation	Air evac confirmation	As required	As required	HF secure	Priority	AECC	
MIJI	Components	As required	As required	E-mail	Immediate	JTF J-6, J-3, J-2	Components
Frequency Interference Report	Components	As required	As required	E-mail	Immediate	JTF J-6	Components
Comm Spot	Components	As required	As required	E-mail	Priority	JTF J-6	Components
Comm Status Summary Report	Components	2400	0200	E-mail	Routine	JTF J-6	
Comm Status Summary Report	JTF J-6	2400	0600	E-mail	Routine	CINC	Components
Bead Window Report	Components	As required	As required	E-mail	Immediate	JTF J-6	Components

9. Orders

a. The CJTF issues guidance and direction in the form of warning orders (WARNORD), FRAGO, execute orders (EXORD), OPORD, and other directives.

The JTF JOC is the focal point for disseminating orders.

b. Orders handoff from the planner to the JOC for execution is a critical element of IM. It is essential that the personnel

responsible for executing the plan have a thorough understanding of the plan. To achieve this level of understanding, a representative from the planning element presents the plan, with supporting synchronization and decision support matrix, to the J-3 current operations and JOC personnel before execution.

10. Briefings and Meetings

a. CJTF Daily Update Brief. The CJTF daily update brief is normally conducted once daily to update the commander on current operations, future, and long range plans; however, the update briefing is conducted as required. The update briefing's purpose is providing the CJTF with analyzed information essential for decisionmaking and synchronizing the efforts of the JTF. A secondary purpose is efficient cross-leveling information within the staff. Brevity, clarity, and a cross-functional analysis of the battlespace are the goals of the CJTF brief.

(1) Suggested briefing sequence (other personnel added as required):

<u>Briefing</u>	<u>Responsibility</u>
Introduction	J-3
Fused Current Operations Update	J-2/J-3
Targeting/ATO Update	J-3 Air
Future Operations Plans	J-3/J-5
Long Range Plans/Political-Military	J-5
As Required	Special Staff
Issues	Component LNO
Issues	Chief of Staff
Conclusion	J-3

(2) Recommended CJTF briefing slides (others added as required):

<u>Slide Title</u>	<u>Responsibility</u>
Current C/D-Day	J-3
Current Operational Phase	J-3
Current Operations Situational Assessment	J-2/J-3
Significant Activities	J-2/J-3
ATOs (Current, Next 24 Hours, Next 72 Hours)	JFACC
Future Operations in Planning	J-3/J-5
Sequels/Transition Plans in Planning	J-5

(3) Recommended Briefing Slide Preparation:

(a) Use black letters on a white background. When building slides, you should not have your "SLIDE MASTER" built with your unique slide requirements for your joint directorate.

(b) Submit slides to the J-3 current operations briefing officer no later than 1 hour before the scheduled brief.

(c) Provide a copy of the commander's daily brief to the JOC operations chief to post to the JTF home page.

b. Chief of Staff Brief. Conduct this briefing once daily or as directed. The briefing's purpose is ensuring that staff directorate efforts are coordinated. Principal staff directors, special staff officers, liaison officers, and others as directed attend the briefing.

(1) The following is a recommended briefing order:

<u>Briefing</u>	<u>Responsibility</u>
Introduction	J-3
Intelligence	J-2
Public Affairs	PAO
Operations	J-3
Future Operations	J-3
Plans	J-5
Logistics	J-4
Communications	J-6
Personnel	J-1
Issues	Special Staff Officers
Issues	LNOs
Closing Remarks	Chief of Staff

(2) Plans Synchronization Meeting. Recommend the Future Operations Planning Chief chair a daily plans synchronization meeting. The purpose is ensuring future and long-range planning efforts synchronize with the current operational situation and prioritizing supporting branch plans in accordance with the current situation. Representatives from J-3 current operations, J-5 plans, and staff directorates should attend the meeting.

11. Internal Policies and Procedures

a. AUTODIN Messages.

(1) The JOC monitors incoming message traffic and posts messages to an incoming message newsgroup, web site, etc.

Track messages by the date-time-group (DTG), originator, subject, or key words describing message content. Using an approved joint message handling system or other spreadsheet/AMHS/web page similar to the example in Table IV-4, users can use a “FIND” command to locate messages related to a subject or key word reference.

(2) Messages are available to and manageable by anyone with an e-mail account. Each directorate establishes internal message handling procedures to manage incoming and outgoing messages on the appropriate web page and/or newsgroup.

(3) The IMP should address AUTODIN message procedures to include release authority, hard copy and soft copy requirements, and DTG assignments.

(4) Staff directorate duties include message review, reading files, suspense assignment, and coordinating activities. Suspense control procedures consist of assigning, copies for distribution, and reviewing status. Maintain a message log for both incoming and outgoing messages.

(5) Each directorate is responsible for maintaining copies of outgoing/incoming correspondence and suspense items. Submit messages through the appropriate staff director or the JTF chief of staff, then forward to the communications center for release. Provide the drafter a comeback copy of all approved and released outgoing messages. The chief of staff reviews the outgoing messages requiring CJTF and JTF review.

b. Master Suspense Action Log. The JOC maintains a suspense log (Table IV-5). Based on JOC chief assignment of OPR and office(s) of collateral responsibility (OCR), the JOC forwards messages to the OPR/OCR for action. The Master Suspense Action Log contains the following entries: tasking agency, OPR, OCR, suspense time,

close-out time, and a brief summary of the tasking. The following instructions apply to the sample Master Suspense Action Log:

(1) Action Item. The message (MSG) or newsgroup article establishing a JTF task or requirement.

(2) Received. DTG the JOC receives the tasking.

(3) Tasked By: Originator of the tasking. Unless otherwise directed, submit responses to the originator.

(4) OPR. The JTF directorate or staff agent responsible for completing the tasking.

(5) OCR: The JTF directorate or staff agency assigned to assist the OPR in completing the assigned tasking.

(6) Suspense. DTG to complete the tasking and post the results to the originator.

(7) Close Out. Actual completion DTG of the tasking.

(8) Task Description. Brief description of the tasking.

c. JTF Significant Event Log. Table IV-6 is an example of an official chronological account of the activities of a JTF. The Significant Events Log, is a running account of JTF significant events. The JOC maintains the log. Instructions for completing the sample log follows:

(1) Time. Time the JOC notes or receives a report of the event.

(2) Notified. Key personnel the JOC chief notified.

(3) Event Description. A brief description of the event. If a follow-on report, refer to DTG of original report.

d. JTF Phone and E-Mail Directory. The JTF and components J-6 or equivalent should publish a phone and e-mail directory (preferably on the JTF's web site on the SIPRNET). The directory contains a brief description of available communications means, instructions on use, and a listing of staff functions with telephone numbers and e-mail addresses. Publish the directory on an appropriate electronic medium (that is, LAN, web page, etc.). Table IV-7 contains a sample directory listing.

12. Multinational Procedures

The JTF establishes procedures for data transfer between the JTF, multinational components, and other agencies. The JTF establishes a multilevel security (MLS) concept of operation for the specific "how-to" for data transfer. Develop information sharing/disclosure policies in accordance with DOD and/or approved multinational policy or procedures. Handle multinational procedures for transferring data dealing with sensitive compartmented information through SSO channels.

Table IV-4. Sample JOC Message Log

DTG	ORIGINATOR	SUBJECT	KEYWORDS		
141752Z JUN 98	CINCUSACOM/J3	WARNING ORDER			
171420Z JUN 98	CINCUSACOM/J3	WARNING ORDER TWO	TASKINGS	CCIR	
181839Z JUN 98	CINCUSACOM/J3	WARNING ORDER THREE	JTF 780	INTENT	
190900Z JUN 98	CINCUSACOM/J3	PLANNING ORDER (PART ONE)	PLANNING GUID	TASKINGS	FORCES
191910Z JUN 98	CINCUSACOM/J3	PLANNING ORDER (PART TWO)	LIFT ALLOCATION	CCIR	LOGISTICS
191530Z JUN 98	CJTF 780	WARNING ORDER NUMBER ONE	COMPONENTS	COMPONENTS	MISSION
192042Z JUN 98	CJTF 788	EXTEND BOUNDARIES OF JOA	JOA	JSOTF	
201345Z JUN 98	CJTF 788	CONTROL OF PSYOP/CA	PSYOPS	CIVIL AFFAIRS	C2
201610Z JUN 98	CTF 785	KEY PERSONNEL LISTING	C2	PHONE	
201810Z JUN 98	CTF 785	JOA MODIFICATION	JOA		
202200Z JUN 98	CJTF 780	WARNORD TWO	TENTATIVE COAS	PLANNING GUIDE	DEPLOYED HQ
211524Z JUN 98	CTF 785	CARRIER AIR WING MODIFICATION	AIR WING		
211830Z JUN 98	CTF 785	REQ FOR ADT'L MIGRANT VESSELS	MIGRANTS		
212320Z JUN 98	CTF 785	CHOP COGARD FORCES	COGARD	MIGRANTS	
231700Z JUN 98	CJTF 788	COURSE OF ACTION (CONOPS)	PHASES	JSOTF	CONOPS
231720Z JUN 98	CJTF 788	PATROL CRAFT TACON SHIFT	COGARD		JSOTF
232035Z JUN 98	CJTF 788	MESSAGE CORRECTION	231700Z JUN 96	JSOTF	CONOPS
241226Z JUN 98	CTF 785	ASSGNM'T OF COGARD & USN	JTF 780	COGARD	USN
241426Z JUN 98	CJTF 780	FRAG ORDER TWO	MIGRANT CAMP	CVBG	MEU/ARG
280257Z JUN 98	CJTF 780	PLANNING INFORMATION	ROCK DRILL		
280335Z JUN 98	CJTF 780	FORCE DEPLOYMENT EXERCISE	DEPLOYMENT		
281910Z JUN 98	CTF 789	JFACC/AFFOR BBS	JFACC	AFFOR	ACP
282157Z JUN 98	CJTF 780	INTENT FOR IW IN PHASE III	IW	PHASES	
300115Z JUN 98	CTF 783	REQUEST FOR GUIDANCE	FOB	SAR	MEU
011844Z JUL 98	CJTF 780	SOTA REQUEST CHANGE ONE	SIGINT		
011600Z JUL 98	CTF 785	OPERATIONS TASK SUBMISSION	JFMCC		

Table IV-5. Sample Master Suspense Action Log

ACTION ITEM	RECEIVED	TASKED BY	OPR	OCR	SUSPENSE	CLOSE OUT	TASK DESCRIPTION
MSG 190337Z FEB 97	192330Z FEB 97	CINCUSAREUR J-3	J-3	J-4	221200Z FEB 97		IDENTIFY FORCE REQUIREMENTS FOR RAMP UP TO 56,000 MIGRANTS
NG 02/19/97 1536	191536Z FEB 97	CINCUSAREUR J-4	J-4		192400Z FEB 97	192259Z FEB 97	STATE EXPECTED CONSUMPTION RATE OF CLASS I
MSG 201128Z FEB 97	201430Z FEB 97	CINCUSAREUR J-3	J-3		211200Z FEB 97	211132Z FEB 97	DEVELOP COAS FOR SEVERE WEATHER EVACUATION
	181320Z FEB 97	CINCARLANT J-2	J-2		19 1200Z FEB 97	191200Z FEB 97	REQUEST CONSIDER ALTERNATIVES FOR MIGRANT TREATMENT BY DOD AND NON-DOD PERSONNEL
NG 02/19/97 0334	190338Z FEB 97	CINCARLANT J-4	J-4		201200Z FEB 97	201002Z FEB 97	REQUEST FOR LAYOUT OF MIGRANT AND JTF CAMP, REQUEST COA FOR DESTRUCTIVE WEATHER RELOCATION
NG 02/19/97 1826Z	191832Z FEB 97	CINCARLANT CAT	J-4				ASSESS FACILITIES AVAILABLE ON NAVBASE FOR HURRICANE (CAT I) PROTECTION

Table IV-6. Sample JTF Significant Events Log

TIME	NOTIFIED	EVENT DESCRIPTION
121300Z FEB 97	CJTF, Chief of Staff	JCS WARNING ORDER DIRECTING CINCSOUTH TO BEGIN MIGRANT OPS PLANNING
180300Z FEB 97	CJTF, J-3	CINCSOUTH ACTIVATES JTF 160 AND DIRECTS COMMENCEMENT OF MIGRANT OPS
181240Z FEB 97	J-3, J-4	M/V ELVA II STRUCK PILINGS ON CALLAN RR BRIDGE. HARBOR CLOSED TO ALL TRAFFIC UNTIL FURTHER NOTICE
181348Z FEB 97	CJTF, J-4	PRESTAGED RATIONS AND WATER SUPPLIES HAVE BEEN CONTAMINATED. CURRENT SUPPLY LEVELS ESTIMATED AT 10 DAYS.
191210Z FEB 97	CJTF	ATTEMPTED MURDER AND RAPE IN CAMP ALPHA
191624Z FEB 97	J-4	COMNAVSTA IMPLEMENTS WATER RATIONING PROCEDURES
200405Z FEB 97	CJTF	FIRE IN MIGRANT VILLAGE CAMP ALPHA, 3 MIGRANTS SEVERELY BURNED FIGHTING FIRE. FIRE EXTINGUISHED BY CAMP FIRE TEAM AND NAVSTA FIRE DEPARTMENT AT 0630Z

Table IV-7. Sample JTF Phone and E-Mail Directory

BILLET/USER	DEVICE	SECURE YES/NO	DSN	COMMERCIAL	TACTICAL	E-MAIL	REMARKS
JTF 780							Home Page http://JTF780
CJTF	STU-III FAX DSVT	Yes Yes No	836-6545 836-6332	(757) 322-6545 (757) 322-6332	201-4201-850	J00	
DCJTF						J01	
CHIEF OF STAFF						J00COSf	
J-1							
J-2							
J-3							
J-4							
J-5							
J-6							
COMMANDER	STU-III FAX DSVT DNVT	Yes Yes No No			201-4201-241 201-4201-242		
ARFOR							Home Page http://ARFOR
MARFOR							Home Page http://MARFOR
AFFOR							Home Page http://AFFOR
NAVFOR							Home Page http://NAVOR

INFORMATION AND INFORMATION SYSTEM PROTECTION

We have evidence that a large number of countries around the world are developing the doctrine, strategies, and tools to conduct information attacks on military-related computers.

John M. Deutch, Director, CIA
Washington Post, 26 June 1996

1. Background

a. Networks and information systems are high-value targets to the enemy and must be adequately protected and defended to maintain the integrity of the joint force C2 infrastructure. Increasing reliance on automated information systems for IM is a JTF's "Achilles Heel" if taken advantage of by an adversary. Mission accomplishment depends on protecting and defending information and information systems from destruction, disruption, corruption, and safeguarding from intrusion and exploitation. Everyone should assume their information and information system is a target. Therefore, all users share responsibility for adequately protecting and defending friendly information and information systems.

b. Protection and defense of information and information systems are accomplished through aggressive application of information assurance measures. The predominant means to apply information assurance is through INFOSEC, which includes intrusion detection, effect isolation, and incident reaction to restore information and system security. Maintain vigilance when using any information medium or communications system. The dynamic nature of the information environment requires well-developed information assurance programs to ensure effective IM.

2. Threats to IM

a. The IM plan must anticipate internal and external threats including—

(1) Hackers (inside or outside the JTF) with limited support and motives to organized and financially backed countries or groups.

(2) Disgruntled system users.

(3) Poor communications security (COMSEC), computer security (COMPUSEC), and OPSEC practices.

(4) Viruses (malicious code).

(5) Unauthorized/unintentional disclosure of data. This threat increases proportionally to the JTF's use of automation.

(6) Corruption of data. An insidious method of deception, if undetected, leads to faulty guidance, coordination, decisionmaking, and execution.

(7) Physical disruption or denial of communications. Threats that may be generated internally or externally.

(8) Terrorist(s) groups.

(9) State sponsored information warfare (IW) attacks.

b. Even easily identified and detected threat techniques are difficult to counter. Others may not be detectable or in place but not activated. Examples of threat techniques are—

(1) Masquerading or attempting to gain access by posing as an authorized user.

Password selection, use, and protection are vital to counter these intrusions.

(2) Spoofing or inserting data causing a system to inadvertently disclose information or data.

(3) Employing electronic warfare by using electromagnetic energy, causing denial of service and corruption of data. Electromagnetic pulses can corrupt and destroy data stored on magnetic media and damage software and hardware.

(4) Providing signals intelligence (SIGINT) information supporting other threats. This provides insight into communications infrastructure and information transfer techniques.

(5) Disrupting planning and operations by substitution and modification. This is the process of modifying or substituting false data or information, with the objective of influencing plans or operations causing users to question the integrity of their information.

(6) Physically attacking facilities resulting in the loss of information connectivity.

(7) Gaining unauthorized access to information processing and transfer systems providing access to friendly information. Typically, knowledge of an organization's systems, procedures, and security barriers is required.

3. Defensive Information Operations

Defensive information operations (a subset of information operations) are actions to protect and defend one's own information and information systems. JTF personnel form an essential line of defense in the way they use office automation and networks. Bring unusual occurrences to the attention of the individuals responsible for defense of information and information systems. Defensive information operations integrate and coordinate policies and

procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive information operations actions include—

a. Determining what data adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information.

b. Selecting and execute measures to eliminate or reduce the vulnerabilities of friendly actions to adversary exploitation.

c. Identifying critical information resources, then taking all possible measures to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto equipment and telecommunications systems.

d. Installing and properly using cryptosystems.

e. Using physical measures necessary to safeguard classified equipment, material, and documents from access or observation thereof by unauthorized persons.

f. Protecting transmissions from interception and exploitation by means other than cryptoanalysis.

g. Protecting capabilities against intrusion, damage, and exploitation.

h. Using warning banners.

i. Using password protected screen savers.

j. Safeguarding passwords. All passwords will—

(1) Be alphanumeric and a minimum of 8 characters.

(2) Be changed regularly.

k. Using configuration controls. J-6 personnel, according to security directives and configuration management controls, are the only personnel authorized to direct changes to the system. This includes making any hardware or software changes.

l. Using information storage procedures.

(1) Store classified data on floppy disks or tapes and secure when not in use or on secure network drives. Do not store classified data on the fixed hard drive unless the workstation is located in a certified and approved area.

(2) Label removable data storage media with the appropriate classification. Examples are the SF 710 (1-87) UNCLASSIFIED Sticker (Green) and the SF 707 (1-87) SECRET Sticker (Red). Classify removable data media at the highest level authorized for that computer system and mark appropriately.

(a) Label floppy diskettes with appropriate security label.

(b) Mark all magnetic media, even with deleted or erased files with the highest level of classification.

(c) Follow the same security rules for floppy disks as used for working 'paper' copies. If the paper working copy requires an accounting and control number, then the diskette will also. See J-6 INFOSEC staff for information on accounting and control of your diskettes. Be sure to perform routine inventories on all disks, tapes, and compact disks read only memory (CD-ROMs).

(3) Use proper classified mailing and/or courier handling procedures for transferring classified magnetic media and CD-ROMs.

(4) Develop procedures for the proper method of releasing classified information.

(5) Reuse disks or tapes at the same classification level or higher. If the disk or tape must be used at a lower classification level, approved methods for clearing, overwriting, or purging data from storage media must be used.

m. Checking for viruses. Introduction of viruses (malicious code) can be from outside or within the organization. Current server-based antivirus software does not intercept viruses in attachments. Only after an attachment is "saved as" (decrypted) does virus scanning occur. Individuals should check for viruses on their workstation by running antivirus software at each shift change. Establish procedures directing users to scan all attachments after saving. The procedures should also outline what the individual does if they discover a virus. Viruses reside in three tiers: server, networked workstations, and diskettes. All members of the JTF should use available antivirus software and comply with the following procedures:

(1) The first tier is the server level. Conduct automatic virus scanning of the networked or shared drive. The network system administrator handles the server level and is transparent to the user. The JTF server runs the antivirus software periodically to catch any infected files placed on the shared drive. The JTF J-6 is responsible for server protection.

(2) The second tier is the networked workstation. At this level, the user accomplishes virus detection and elimination by initiating virus detection software or setting the virus scanning software to accomplish automatic system scans at timed intervals.

(3) The third tier is diskettes. Diskettes act as hosts for the virus to travel from machine to machine. Unless you know otherwise, assume diskettes are infected. Always scan diskettes before use. The JTF J-6 will establish a site for conducting virus scanning of incoming diskettes. Never permit JTF personnel to use diskettes

before virus checking. The J-6 will install antivirus software on the LAN in order for users to check files downloaded from newsgroups or e-mail. Liaison officers may bring their own laptop computers. The J-6 should develop procedures for scanning laptop computers before their use in the JTF.

n. Observe the following guidelines for unclassified (NIPRNET) internet use;

(1) Do not process or exchange classified information via the internet.

(2) Grant internet access for users with a valid mission need and for official use only.

(3) Scan all software downloaded from the internet with updated virus detection software.

(4) Do not post WWW pages on JTF systems without approval of J-6 INFOSEC and public affairs staffs. Information exchanged via the internet or WWW is generally unprotected and subject to compromise.

4. Information Destruction

a. Treat electronic records the same as paper records. Records no longer required shall be disposed of in accordance with the provisions of the Federal Records Act (44 USC 21 and 33). Continue appropriate protection for materials identified for destruction until destroyed.

b. Accomplish destruction by means that eliminate the risk of reconstruction of the classified information.

(1) Burn Bags. Place burn bags throughout all workspaces, particularly in areas with printers and copiers. Never locate classified burn bags in close proximity to unclassified waste containers. Users must be aware of the potential to piece together the JTF's operations from minor or seemingly insignificant bits of information. If in doubt, dispose of unneeded materials in a burn bag. Control burn bags in a manner minimizing the possibility of unauthorized removal of the bag or the contents before destruction. When filled, seal burn bags in a manner facilitating the detection of tampering with the bag. Mark sealed bags with an office symbol and the highest classification of the information contained. Keep records of destruction if required.

(2) Magnetic Media Destruction. Special security handling procedures for clearing and/or purging, destroying, and removing of external markings from magnetic media and CD-ROMs are needed to prevent the unintentional disclosure of information. This includes data remnants or traces of information remaining on storage media even after the use of purging procedures. Classified storage media should be destroyed when no longer usable. Contact the JTF help desk for procedures for destroying data storage media.

REFERENCES

Joint

- Department of Defense (DOD) Directive 8000.1, *Defense Information Management (IM) Program*, 27 Oct 92.
- DOD Directive 8910.1, *Management and Control of Information Requirements*, 11 Jun 93
- DOD Directive 5015.2-STD, *Design Criteria Standard for Electronic Records Management Software Applications*, 24 Nov 97
- Corporate Information Management for the 21st Century, A DOD Strategic Plan*, June 1994
- Report by a Panel of the National Academy of Public Administration for the U.S. DOD, *Information Management Performance Measures*, January 1996
- Joint Publication 1-03, *Joint Reporting Structure (JRS) General Instructions*, 10 Jan 94
- Joint Publication 3-13, *Joint Doctrine for Information Warfare*, 9 Oct 98
- Joint Publication 3-56, *Command and Control Doctrine for Joint Operations*, 2nd Draft, 30 Apr 97
- Joint Publication 5-00.2, *Joint Task Force Planning Guidance and Procedures*, 13 Jan 99
- Joint Publication 6-0, *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations*, 30 May 95
- Joint Publication 6-02, *Joint Doctrine for Employment of Operational/Tactical Command, Control, Communications, and Computer Systems*, 1 Oct 96
- CJCSI 3122.01, JOPES Volume I, *Planning Policies and Procedures*, Chapter V.
- CJCSI 3151.01, *Chairman of the Joint Chiefs of Staff Instruction, Global Command and Control System Common Operational Picture Reporting Requirements*, 10 Jun 97
- CJCSI 6510.01B, *Chairman of the Joint Chiefs of Staff Instruction, Defensive Information Operations Implementation*, 22 Aug 97
- CJCSM 6120.01A, *Joint Multi-tactical Digital Information Link Operating Procedures*, October 1997
- Joint Task Force Architecture Specification (JTFAS)*, 13 Apr 94
- Information Management Plan, Unified Endeavor 97-1*, Executive Summary, 18 Nov 96
- Information Management Plan, Unified Endeavor 98-1*, Coordinated Draft, 12 Sep 97
- Framework for Information Management (IDM) Services*, 5 Sep 97
- Joint Force Quarterly, *Rethinking the Joint Doctrine Hierarchy*, Winter 1996-97
- Battlefield Awareness and Data Dissemination (BADD) Advanced Concept Technology Demonstration (BADD ACTD) Management Plan*, 30 Apr 97
- JULLS Long Report, Number 22836-71516 (00010), 8 Mar 96
- JULLS Long Report, Number 12748-78965 (00013), 19 Feb 97

Multiservice

Air Land Sea Application (ALSA), *Information Warfare/Information Operations Study*,
15 Dec 95

Army

Army Digitization Master Plan '96, Chapter 4, Architecture

AR 25-1, *Information Management*, 25 Mar 97

FM 100-5, *Operations*, 14 Jun 93

FM 100-6, *Information Operations*, August 1996

FM 100-7, *Decisive Force: The Army in Theater Operations*, 31 May 95

FM 101-5, *Staff Organization and Operations*, 31 May 97

TRADOC Pam 525-5, *Force XXI Operations, A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century*, 1 Aug 94

TRADOC Pam 525-69, *Concept for Information Operations*, 1 Oct 95

XVIII Airborne Corps, *Joint Task Force Headquarters Standing Operating Procedures*, 1 Dec 96

Marine Corps

MCDP 6, *Command and Control*, 4 Oct 96

Navy

Naval Doctrine Publication 6, *Naval Command and Control*, 19 May 95.

Air Force

Air Force Doctrine Document 1, *Basic Doctrine*, September 1997

Air Force Doctrine Document 2, *Global Engagement, Air and Space Power Organization and Employment*, 28 Sep 98

Air Force Doctrine Document 2-5, *Information Operations*, 5 Aug 98

Air Force Doctrine Document 2-8, *Command and Control (Draft)*

Air Force Manual 37-104, *Information Management*, 1 Jun 95

Air Force Policy Directive 31-4, *Information Security*, 1 Aug 97

Air Force Policy Directive 33-2, *Information Protection*, 1 Dec 96

Air Force Policy Directive 37-1, *Information Management*, 19 Nov 93

GLOSSARY

PART I—ABBREVIATIONS AND ACRONYMS

A

aaslt	air assault
ABN	airborne
ACO	airspace control order
ACP	airspace control plan
ACR	armored cavalry regiment
ADA	air defense artillery
ADP	automatic data processing
ADSI	Air Defense System Integrator
adt'l	additional
admin	administration
AECC	aeromedical evacuation control center
AELT	aeromedical evacuation liaison team
AFDC	Air Force Doctrine Center
AFFOR	Air Force forces
AFI	Air Force Instructions
AFTTP(I)	Air Force Tactics, Techniques, and Procedures (Interservice)
AIS	automated information system
ALSA	Air Land Sea Application Center
AMHS	Automated Message Handling System
AOR	area of responsibility
AR	armor
ARFOR	Army forces
ARG	amphibious ready group
ASAS	All Source Analysis System
ASCII	American Standard Code for Information Interchange
assgnm't	assignment
ATO	air tasking order
AUTODIN	Automatic Digital Network

B

BBS	bulletin board system
BDA	bomb or battle damage assessment

C

C-Day	unnamed day on which a deployment operation commences or is to commence
C2	command and control
C2W	command and control warfare
C3	command, control, and communications
C4	command, control, communications, and computers
C4I	command, control, communications, computers, and intelligence
CA	civil affairs; combat assessment
CAP	crisis action planning

CAT	crisis action team
CCIR	commander's critical information requirements
C-Day	unnamed day on which a deployment operations begins
CDR	commander
CD-ROM	compact disk read only memory
CI	counterintelligence
CIA	Central Intelligence Agency
CINC	commander of a combatant command, commander in chief
CINCARLANT	Commander in Chief, Army Forces Atlantic
CINCSOUTH	Commander in Chief, United States Southern Command
CINCUSACOM	Commander in Chief, United States Atlantic Command
CINCUSAREUR	Commander in Chief, United States Army, Europe
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CJTF	commander, joint task force
Cmd	command
CMO	civil-military operations
CMOC	civil-military operations center
COA	course of action
COE	common operating environment
COGARD	Coast Guard
COLISEUM	Community On-line Intelligence System for End-Users and Managers
COMM	communications
COMNAVSTA	commander naval station
COMPUSEC	computer security
COMSEC	communications security
COMSTAT	communications status
CONOPS	concept of operations
COP	common operational picture
COPM	common operational picture manager
CPS	collaborative (integrated) planning system
CTAPS	contingency theater automated planning system
CTD	common tactical dataset
CTF	combined task force
CTP	common tactical picture
CTPB	common tactical picture board
CTPM	common tactical picture manager
CVBG	carrier battle group

D

DAA	designated approving authority
DA	Department of the Army
D-Day	unnamed day on which operations commence or scheduled to commence
DCJTF	deputy commander, joint task force
DDN	Defense Data Network
Dep	deputy
dept	department
det	detachment
DII	defense information infrastructure

DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISUM	daily intelligence summary
div	division
DMDS	Defense Message Distribution System
DMS	Defense Message System
DNVT	digital nonsecure voice terminal
DOD	Department of Defense
DOS	Department of State; disk operating system
DRSN	Defense Red Switch Network
DSN	Defense Switched Network
DSVT	digital subscriber voice terminal
DTG	date-time group

E

E-5	enlisted pay grade level 5
E-7	enlisted pay grade level 7
ech	echelon
EEFI	essential elements of friendly information
EI	essential elements of information
ELINT	electronic intelligence
e-mail	electronic mail
EPW	enemy prisoner of war
evac	evacuation
EWO	electronic warfare officer
EXORD	execute orders

F

fac	facility
FAX	facsimile
FDESC	force description
FFIR	friendly force information requirements
FM	Field Manual
FOB	forward operations base
FP	force protection
frag	fragmentary
FRAGO	fragmentary order

G

G-1	Army or Marine Corps component manpower or personnel staff officer (Army division or higher staff, Marine Corps brigade or higher staff)
G-2	Army or Marine Corps component intelligence staff officer (Army division or higher staff, Marine Corps brigade or higher staff)
G-3	Army or Marine Corps component operations staff officer (Army division or higher staff, Marine Corps brigade or higher staff)

G-4	Army or Marine Corps component logistics staff officer (Army division or higher staff, Marine Corps brigade or higher staff)
G-5	Army component civil-military operations staff officer
G-6	Army or Marine Corps component signal operations staff officer (Army division or higher staff, Marine Corps brigade or igher staff)
GBS	Global Broadcasting System
GCCS	Global Command and Control System
GENSER	general service (message)
GSA	General Services Administration
GSORTS	global command and control system status of resources and training system

H

HF	high frequency
HQ	headquarters
hrs	hours
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocols

I

I/W	indications and warnings
IATO	interim authority to operate
IC	internet chat
IDM	information dissemination management
IER	information exchange requirements
IIR	intelligence information report
IM	information management
IMB	information management board
IMO	information management officer
IMP	information management plan
INF	infantry
Info	information
INFOSEC	information security
INFOSYS	information system
intel	intelligence
INTSUM	intelligence summary
IO	information operations
IRC	Internet relay chat
IS	information systems
ISB	intermediate staging base
ISSM	information systems security manager
ISSO	information systems security officer
IW	information warfare

J

J-1	Manpower and Personnel Directorate of a joint staff
J-2	Intelligence Directorate of a joint staff
J-3	Operations Directorate of a joint staff

J-4	Logistics Directorate of a joint staff
J-5	Plans Directorate of a joint staff
J-6	Command, Control, Communications, and Computer Systems Directorate of a joint staff
JAC	joint operations center/joint intelligence support element assessment cell
JASC	Joint Actions Steering Committee
JCATF	joint crisis action team function
JCCC	joint communications control center
JCMOTF	Joint Civil-Military Operations Task Force
JCS	Joint Chiefs of Staff
JDISS	Joint Deployable Intelligence Support System
JFACC	joint force air component commander
JFC	joint force commander
JFLCC	joint force land component commander
JFMCC	joint force maritime component commander
JIB	Joint Information Bureau
JIC	Joint Intelligence Center
JISE	joint intelligence support element
JMCIS	Joint Maritime Command Information System
JMRO	Joint Medical Regulating Office
JOA	joint operations area
JOC	Joint Operations Center
JOCC	Joint Operations Center Chief
JOPEs	Joint Operation Planning and Execution System
JP	joint publication
JPG	joint planning group
JPOTF	joint psychological operations task force
JRS	joint reporting structure
JSOTF	joint special operations task force
JSRC	joint search and rescue center
JTA	joint terminal architecture
JTCB	Joint Targeting Coordination Board
JTF	joint task force
JULLS	Joint Universal Lessons Learned System
JWG	joint working group
JWICS	Joint Worldwide Intelligence Communications System
L	
L	local
LAN	local area network
LNO	liaison officer
LOGSITREP	logistic situation report
LTIOV	latest time information of value
M	
M/V	motorized vessel
MACOM	major Army command
MAJCOM	major command (USAF)
MARFOR	US Marine Corps forces

MCCDC	Marine Corps Combat Development Command
MCDP	Marine Corps Doctrinal Publication
MCPDS	Marine Corps Publication Distribution System
MCRP	Marine Corps Reference Publication
MCS/P	Maneuver Control System Phoenix
Mech	mechanized
med	medical
METOC	meteorological and oceanographic
MEU	Marine expeditionary unit
MEU/ARG	Marine expeditionary unit/amphibious ready group
mgt	management
MIJI	meaconing, interference, jamming, intrusion
MILSTIP	military standard requisitioning and issue procedures
MLS	multilevel security
MOA	memorandum of agreement
MOTRE/TRAP	mobile tactical receive equipment/tactical related applications
MSC	major subordinate command
MSEL	master scenario events list
MSG	message
MTF	message text formats
MTTP	multiservice tactics, techniques, and procedures

N

N/A	not applicable
NATO	North Atlantic Treaty Organization
NAVSOP	Naval Standard Operating Procedures
NAVFOR	US Navy forces
NAVSTA	naval station
NBC	nuclear, biological, and chemical
NEO	noncombatant evacuation operation
NFA	no-fire area
NG	newsgroup
NGO	nongovernmental organization
NIMA	National Imagery and Mapping Agency
NIPRNET	Nonsecure Internet Protocol Router
NLT	not later than
NSA	National Security Agency
NSO	network security officer
NWDC	Navy Warfare Development Command
NWP	Naval Warfare Publication

O

O-5	officer pay grade level 5 (lieutenant colonel)
OCR	office of collateral responsibility
OPCON	operational control
OPFOR	opposing force
OPLAN	operation plan
OPNOTE	operations note
OPORD	operation order
OPR	office of primary responsibility

OPS	operations
OPSEC	operations security
OTH	over the horizon
P	
PAO	Public Affairs Office; public affairs officer
PIR	priority intelligence requirements
PLA	plain language address
PM	provost marshal
POC	point of contact
POL	petroleum, oils, and lubricants
PSYOP	psychological operations
PVO	private voluntary organization
R	
RDA	research, development, and acquisition
RECCE	reconnaissance
RECON	reconnaissance
req	requirement
RFA	restricted fire area
RFI	request for information
ROE	rules of engagement
rpt	report
RR	railroad
S	
SAM	surface-to-air missile
SAR	search and rescue
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SCUD	surface-to-surface missile system
SIGINT	signals intelligence
SIMLM	single integrated medical logistics management
SIPRNET	Secret Internet Protocol Router Network
SITREP	situation report
SJA	Staff Judge Advocate
SMG	special mail guard
SOF	special operations forces
SOP	standing operating procedures
SOTA	signals intelligence operational tasking authority
SSO	special security officer
ST&E	security test and evaluation
STO	special technical operations
STU-III	secure telephone unit III
T	
TACON	tactical control
TARGET	Theater Analysis and Replanning Graphical Execution Toolkit

TASO	terminal area security officer
TDBM	technical data base management
TIM	theater information management
TMD	theater missile defense
TPFDD	time-phased force and deployment data
TRADOC	United States Army Training and Doctrine Command
TRAP	tactical receive equipment and related applications
TS	top secret
T-SCIF	tactical sensitive compartmented information facility
TSCO	top secret control officer
TTP	tactics, techniques, and procedures

U

UE	Unified Endeavor
URL	universal reference locator
US	United States
USC	United States Code
USMTF	United States message text format
USN	United States Navy
USTRANSCOM	United States Transportation Command

V

VTC	video teleconferencing
------------	------------------------

W

w	with
WARNORD	warning order
WHNS	wartime host-nation support
WMD	weapons of mass destruction
WWW	world wide web
WX	weather

Z

Z	ZULU
ZULU	time zone indicator for Universal Time

PART II – TERMS AND DEFINITIONS

battle rhythm. See daily operations cycle.

commander's critical information requirements (CCIR). Information required by the commander that directly affects his decisions and dictates the successful execution of operational or tactical operations. CCIR normally result in the generation of three types of information requirements: priority intelligence requirements, essential elements of friendly information, and friendly force information requirements. (FM 101-5-1, MCRP 5-2A)

common operational picture (COP). The COP is the integrated capability to receive, correlate, and display a common tactical picture (CTP), including planning applications and theater-generated overlays/projections (i.e., Meteorological and Oceanographic (METOC), battleplans, force position projections). Overlays and projections may include location of friendly, hostile, and neutral units, assets, and reference points. The COP may include information relevant to the tactical and strategic level of command. This includes, but is not limited to, any geographically oriented data, planning data from JOPES, readiness data from SORTS, intelligence (including imagery overlays), reconnaissance data from the Global Reconnaissance Information System (GRIS), weather from METOC, predictions of nuclear, biological, and chemical (NBC) fallout, and air tasking order (ATO) data. (CJCSI 3151.01)

common tactical dataset (CTD). The CTD is a repository of data that contains all the information available to the JTF that will be used to build the COP and CTP. The CTD is not fused, correlated, or processed data in the sense that the information has been scrutinized by the COP manager (CCM) or track managers for time value, redundancy, or conflicts. However, the CTD may contain processed intelligence data. The CTD is a major subcomponent of the COP and refers to: the CINC designated repository for current battlespace information including disposition of hostile, neutral, and friendly forces as they pertain to US and multinational operations ranging from peacetime through crisis and war for the entire area of responsibility (AOR). Upon discretion of the CINC, the CTD may be a logical database vice physical if there are several JTFs or activities that will necessitate COP reporting. In these cases there may be more than one location of database storage. (CJCSI 3151.01)

common tactical picture (CTP). The CTP is derived from the CTD and other sources and refers to the current depiction of the battlespace for a single operation within a CINC's AOR including current, anticipated or projected, and planned disposition of hostile, neutral, and friendly forces as they pertain to US and multinational operations ranging from peacetime through crisis and war. The CTP includes force location, real time and non-real-time sensor information, and amplifying information such as METOC, SORTS, and JOPES. (CJCSI 3151.01)

COP correlation site (CCS). The CCS is the CINC-designated location where all data in the COP is received, correlated, managed, and disseminated by the CCM. (CJCSI 3151.01)

daily operations cycle. The schedule of significant recurring events of the JTF HQ staff. The JTF chief of staff normally establishes this to deconflict the JTF staff schedule. This schedule allows JTF staff members to anticipate when information is required and backward plan to ensure inputs are available when needed.

defense information. The shared or interconnected system of computers. (FM 100-6).

Global Information Environment. All individuals, organizations, or systems, most of which are outside the control of the military or National Command Authorities, that collect, process, and disseminate information to national and international audiences. (FM 100-6)

IM board (IMB). The focal point for coordinating information management within a JTF HQ. Chaired by the JTF IMO, this board operates under the supervision of the JTF chief of staff, or other appropriate staff directorate, as best meets the JTF requirements. This board should be composed of the senior IMO from each staff section, component, and supporting agency. The board actively resolves all cross-functional information management issues, convening on an as required basis.

information filter. Accessing the value of information and culling out that which is not pertinent or important.

information flow. Term used to describe movement of information.

information fusion. The logical blending and integration of information from multiple sources into an accurate, concise, and complete summary.

information management (IM). The processes by which information is obtained, manipulated, directed, and controlled. IM includes all processes involved in the creation, collection and control, dissemination, storage and retrieval, protection, and destruction of information.

information operations (IO). Actions taken to affect adversary information and information systems while defending one's own information and information systems. (Joint Pub 3-13)

information security (INFOSEC). The protection of information and information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. (Joint Pub 3-13)

JOC/JISE Assessment Cell (JAC). An optional cell to maintain operational awareness of the battlespace through continuous fusion and assessment of all-important friendly and enemy information.

Military Information Environment. The environment contained within the global information environment, consisting of information systems and organizations—friendly and adversary, military and nonmilitary—that support, enable, or significantly influence a specific military operation. (FM 100-6)

query. As applied to JOPES permissions, “query” is one of the ten functional permissions granted users. The permission is limited to retrieving and viewing information on the terminal display screen. The other primary functions allow users to update, perform database management and scheduling functions, and print charts and reports. (Adapted from JOPES User's Manual)

request for information (RFI). 1. Any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. A request for information can be initiated to respond to operational requirements and will be validated in accordance with the theater command's procedures. 2. The National Security Agency/Central Security Service uses this term to state ad hoc signals intelligence requirements. (Joint Pub 1-02).

INDEX

C

CCIR iv, vi, vii, II-3, III-4, III-5, III-6,
III-7, IV-1, IV-5, IV-14
CJTF I-1, I-2, I-4, I-5, II-3, II-4, III-4, III-12,
IV-1, IV-5, IV-7, IV-10, IV-11, IV-12,
IV-14, IV-15
Cognitive Hierarchy iii, iv, I-2, I-3, I-4
Commander, Joint Task Force (*see* CJTF)
Commander's Critical Information
Requirements (*see* CCIR)
Common Tactical Picture Board (*see* CTPB)
Common Tactical Picture Manager (*see*
CTPM)
CTPB iii, II-5, III-2
CTPM II-5, III-2, IV-4

D

Defensive Information Operations iv, V-2,
References-1

E

Electronic Mail (*see* E-mail)
E-mail ii, v, vi, vii, II-1, II-3, II-4, II-5, III-1,
III-3, III-8, III-9, III-10, III-13, IV-1, IV-3,
IV-8, IV-9, IV-10, IV-12, IV-13, IV-15,
V-4

G

GBS iv, III-12, III-13
GCCS iv, vi, vii, III-1, III-3, III-9, IV-1,
IV-4, IV-9, IV-10, References-1
Global Broadcasting System (*see* GBS)
Global Command and Control System (*see*
GCCS)

I

IMB iii, II-4, II-5
IMO i, iv, I-2, I-5, II-3, II-4, II-5, II-6, III-3,
III-7, III-11, III-12
IMP i, iii, vi, I-2, I-5, II-3, II-4, II-5, II-6,
III-3, III-4, III-5, III-6, III-7, III-12, IV-12,
References-1

Information Destruction iv, V-4
Information Flow iii, v, vi, vii, I-4, I-5, II-1,
II-4-II-5, III-1, III-12-III-13, IV-2, IV-6
Information Management Board (*see* IMB)
Information Management Officer (*see* IMO)
Information Management Plan (*see* IMP)
Internet Relay Chat (*see* IRC)
IRC III-9

J

JAC iv, IV-5, IV-6
JISE iv, vi, II-4, II-5, III-12, IV-1, IV-5,
IV-7
JOC iv, v, vi, II-4, II-5, III-6, III-7, III-10,
IV-1, IV-5, IV-6, IV-7, IV-10, IV-11, IV-12,
IV-13, IV-14
Joint Intelligence Support Element (*see*
JISE)
Joint Operations Center (*see* JOC)
Joint Intelligence Support Element
Assessment Cell (*see* JAC)
Joint Task Force Chief of Staff (*see* JTF
Chief of Staff)
Joint Task Force Common Tactical Picture
Board (*see* JTF Common Tactical Picture
Board)
Joint Task Force Daily Operations Cycle
(*see* JTF Daily Operations Cycle)
Joint Task Force Information Management
Officer (*see* JTF IMO)
Joint Task Force Web Administrator (*see*
JTF Web Administrator)
Joint Task Force Web Grandmaster (*see*
JTF Web Grandmaster)
JTF Chief of Staff II-3, III-11, III-12, IV-6,
IV-12
JTF Common Tactical Picture Board iii,
II-5
JTF Daily Operations Cycle iv, IV-6
JTF IMO iv, I-5, II-3, II-4, II-5, II-6, III-3,
III-7, III-11
JTF Web Administrator II-4, II-5, II-6,
III-3
JTF Web Grandmaster II-3, II-6

L

LAN iv, II-3, III-1, III-8, III-11, IV-13, V-4
Local Area Network (*see* LAN)

M

Multinational Procedures iv, IV-13

R

Request for Information (*see* RFI)

RFI iv, vi, vii, I-2, II-3, II-5, III-1, III-2,
III-4, III-5, III-6, III-7, III-10, IV-1, IV-2,
IV-3, IV-4, IV-8

V

Video Teleconferencing (*see* VTC)
VTC iv, v, II-1, III-7, III-11, III-12, IV-7

W

Webmaster II-3, II-5, II-6

**FM 101-4
MCRP 6-23A
NWP 3-13.1.16
AFTTP(I) 3-2.22
8 April 1999**

BY ORDER OF THE SECRETARY OF THE AIR FORCE

**TIMOTHY A. KINNAN
Major General, USAF
Commander
Headquarters Air Force Doctrine Center**

Air Force Distribution: F

**FM 101-4
MCRP 6-23A
NWP 3-13.1.16
AFTTP(I) 3-2.22
8 APRIL 1999**

DISTRIBUTION:

Active Army, Army National Guard, and U.S. Army Reserve: To be distributed in accordance with the initial distribution number 115770, requirements for FM 101-4

